ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2021-28

July 30, 2021

CALGARY POLICE SERVICE

Case File Number 006357

Office URL: www.oipc.ab.ca

Summary: The Applicant made a request to the Calgary Police Service (the Public Body) for the following:

> Any and all information, including but not limited to witness statements, reports, video and audio tape surveillance of a May 18, 2016 occurrence under CPS action #16211995. I specifically require a copy of the 7-11 video.

The Public Body conducted a search for records and responded to the Applicant. It severed information under sections 17 (disclosure harmful to personal privacy), 20(1)(g) and (m) (disclosure harmful to law enforcement) and 24(1)(b) (advice from officials).

The Adjudicator confirmed the Public Body's decision to apply section 17 to withhold information, but for cell phone numbers and direct lines of Crown prosecutors, which she considered were subject to section 25 (disclosure harmful to economic and other interests of a public body). The Adjudicator asked the Public Body to reconsider its decision to sever information regarding a Crown prosecutor's exercise of discretion by taking into consideration the fact that the Crown prosecutor had communicated the substance of the severed information at an earlier date.

The Adjudicator determined that information regarding the address of the Public Body's spam folder and the information to which it had applied section 24(1)(b) was outside the scope of the access request and was nonresponsive. As a result, she did not order disclosure of this information.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act*, RSA 2000, c. F-25, ss. 10, 17, 18, 20, 24, 25, 72

Authorities Cited: AB: Orders F2007-029, F2019-09, F2020-13, F2021-08

Cases Cited: *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23

1. BACKGROUND

[para 1] The Applicant was a complainant in a criminal assault case. He made an access request to the Calgary Police Service (the Public Body) under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act) for records relating to its investigation of the assault. He requested:

> Any and all information, including but not limited to witness statements, reports, video and audio tape surveillance of a May 18, 2016 occurrence under CPS action #16211995. I specifically require a copy of the 7-11 video.

[para 2] The Public Body conducted a search for responsive records and responded to the Applicant. It severed information from the records under sections 17 (disclosure harmful to personal privacy), sections 20(1)(g) and (m) (disclosure harmful to law enforcement) and 24(1)(a) and (b) (advice from officials).

[para 3] The Applicant requested review by the Commissioner of the Public Body's response to his access request.

II. ISSUES

ISSUE A: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act (duty to assist applicants)?

ISSUE B: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) apply to the information to which the Public Body applied this provision?

ISSUE C: Did the Public Body properly apply section 20(1) of the Act (disclosure harmful to law enforcement) to the information in the records?

ISSUE D: Did the Public Body properly apply section 24(1) of the Act (advice from officials) to the information in the records?

III. DISCUSSION OF ISSUES

ISSUE A: Did the Public Body meet its duty to the Applicant as provided by section 10(1) of the Act (duty to assist applicants)?

[para 4] Section 10(1) of the Act states:

> *10(1) The head of a public body must make every reasonable effort to assist applicants and to respond to each applicant openly, accurately and completely.*

[para 5] In Order F2007-029, the Commissioner made the following statements about a public body's duty to assist under section 10(1):

> The Public Body has the onus to establish that it has made every reasonable effort to assist the Applicant, as it is in the best position to explain the steps it has taken to assist the applicant within the meaning of section 10(1).
>
> . . .
>
> Previous orders of my office have established that the duty to assist includes the duty to conduct an adequate search for records. In Order 2001-016, I said:
>
> > In Order 97-003, the Commissioner said that a public body must provide sufficient evidence that it has made a reasonable effort to identify and locate records responsive to the request to discharge its obligation under section 9(1) (now 10(1)) of the Act. In Order 97-006, the Commissioner said that the public body has the burden of proving that it has fulfilled its duty under section 9(1) (now 10(1)).
> >
> > Previous orders . . . say that the public body must show that it conducted an adequate search to fulfill its obligation under section 9(1) of the Act. An adequate search has two components: (1) every reasonable effort must be made to search for the actual record requested and (2) the applicant must be informed in a timely fashion what has been done.
>
> . . .
>
> In general, evidence as to the adequacy of search should cover the following points:
>
> - The specific steps taken by the Public Body to identify and locate records responsive to the Applicant's access request
> - The scope of the search conducted – for example: physical sites, program areas, specific databases, off-site storage areas, etc.
> - The steps taken to identify and locate all possible repositories of records relevant to the access request: keyword searches, records retention and disposition schedules, etc.
> - Who did the search
> - Why the Public Body believes no more responsive records exist than what has been found or produced

[para 6] In his request for review, the Applicant questioned whether the Public Body had searched for all responsive records. He made no submissions in the inquiry regarding this issue.

[para 7] The Public Body provided the following description of its search through the affidavit of its Disclosure Analyst:

> I am a civilian member of the Calgary Police Service (CPS) where I am employed as a Disclosure Analyst in the Access and Privacy Section. I have been employed in this capacity for nearly 10 years. I have personal knowledge of the facts and matters hereinafter deposed to, save and except where stated to be based upon information and belief and where so stated, I verily believe the same to be true.
>
> On or about March 21, 2017, I was assigned to respond to the access request submitted by the Applicant. The file number assigned to the request was 17-P-0427.
>
> Upon being assigned file 17-P-0427 I reviewed the request and noted that the Applicant was looking for all information, including videos, in relation to a specific case file, that being case file 16211995.
>
> I searched our Sentry database which contains all our police case file reports and located the report for file 16211995. I downloaded the file.
>
> Upon downloading file 16211995 I reviewed the report to determine which CPS members were involved in the files and who the involved parties and witnesses were so I could follow up with the officers and continue my search for records, including the officer notes and any witness statements.
>
> I identified the following officers as being involved in the call: Cst. […], Cst. […] […] and Cst. […]. I made a written request to each of them to provide all of their records, including emails, notes, photos, and videos, related to case file 16211995. I also noted that Cst. […] and his partner, […], were involved in obtaining statements relating to the call so I also made a request for them to provide all of their records relating to case file 16211995. Finally, I requested all records, including video, from […] from the air support unit. In the addition to the officers, I identified one employee member of CPS who was involved in the call. […] was the civilian pilot who flew the helicopter that transported […]. I know from my experience that the pilots in the air support unit do not make records of incidents that occur during their flights and that he would have no responsive records.
>
> Where an officer or employee involved in case file 16211995 advised me they did not have any responsive records, I received an explanation to satisfy myself that a proper search had occurred and that there were no responsive records. […] advised that he was involved only as a backup officer for safety reasons and he had no involvement with the investigation other than attending the scene. He did search his duty notebooks for the relevant timeframe and had no notes.
>
> Similarly, Cst. […], Cst. […] and Cst. […] advised they did not have any records. Cst. […] and Cst. […] noted that the assault investigation was dealt with by a different district than their district and they had no notes or other records relating to the matter.
>
> I conducted a search for records on our CAD (computer aided dispatch) system and downloaded the record of the CAD call. I reviewed the CAD call records to ensure I had identified all of the officers and employees who might have responsive records.
>
> In addition to the searches I conducted of the involved officers and employee, I also conducted a search for records in our Livelink database which is where records such as photographs, officer notes, statements and other documents relating to a file are stored. I searched Livelink by the case file number and downloaded all responsive records.

> I also conducted a search for records in the Evidence and Property Unit. This is where any exhibits relating to a particular matter would be stored. I searched by case file number and received responsive records from the Evidence and Property Unit.
>
> At this point in the processing of this request for records, I had conducted searches of the online police databases that might hold responsive records (Sentry, Livelink, CAD) and collected those records. I had contacted all the involved police officers to collect records directly from them. I also conducted a search and received records from the Evidence and Property Unit. I was satisfied that I had searched all locations where potentially responsive records might reside and that there were no other repositories where responsive records might reasonably be expected to be found.
>
> Prior to finalizing the response to the Applicant's request for records, I reviewed the file with the Senior Disclosure Analyst. She did not identify any additional potential sources of records.
>
> Based on the foregoing I have concluded that there are no other locations where responsive records may be located and that all of the records responsive to the Applicant's request have been located and collected.

[para 8] The Disclosure Analyst's affidavit provides a detailed explanation of the search he conducted and addresses all the points set out in Order F2007-029. In particular, he has satisfactorily explained why he believes no more records exist than have been produced.

[para 9] The Applicant has provided no evidence or explanation as to why he believes additional records exist. While he refers in his request for review to a possibility that records may have been deleted, he has not adduced any evidence what would support this assertion.

[para 10] From the evidence before me, I am satisfied that the Public Body conducted a reasonable search for responsive records and has established that it is likely that no additional responsive records exist. I find that the Public Body met its duty to assist the Applicant.

ISSUE B: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) apply to the information to which the Public Body applied this provision?

[para 11] The Public Body has applied section 17 to withhold names and other information about individuals involved in the case from the Applicant. It also applied section 17 to the cell phone numbers of police officers, although it also applied section 20(1)(m) to withhold this information from some records. I will address the severing of cell phone numbers in my decision in relation to section 20, below.

[para 12] It stated the following regarding its application of section 17:

> There is no basis for suggesting the personal information would further the purpose of subjecting the activities of the Government of Alberta or a public body to scrutiny. No evidence has been submitted by the Applicant that the Redacted Information required to satisfy the following factors:

17(5)(b): the disclosure is likely to promote public health and safety or the protection of the environment;

17(5)(c): the personal information is relevant to a fair determination of the applicant's rights;

17(5)(d): the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people;

17(5)(g): the personal information is likely to be inaccurate or unreliable; or

17(5)(i): the personal information was originally provided by the Applicant.

CPS submits disclosure of the Redactions would constitute an invasion of privacy of the third parties, and the Applicant has not demonstrated the disclosure of the Redactions would not amount to an unreasonable invasion of privacy.

[para 13] Other than to assert in his requests for review and inquiry that he did not believe the Public Body had severed information appropriately, the Applicant did not provide submissions regarding section 17.

[para 14] Section 17 requires a public body to withhold the personal information of an identifiable individual when it would be an unreasonable invasion of the individual's personal privacy to disclose his or her personal information.

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.

[…]

(4) A disclosure of personal information is presumed to be an unreasonable invasion of a third party's personal privacy if

[…]

(b) the personal information is an identifiable part of a law enforcement record, except to the extent that the disclosure is necessary to dispose of the law enforcement matter or to continue an investigation,

[…]

(g) the personal information consists of the third party's name when

(i) it appears with other personal information about the third party, or

(ii) the disclosure of the name itself would reveal personal information about the third party,

[…]

(5) In determining under subsections (1) and (4) whether a disclosure of personal information constitutes an unreasonable invasion of a third party's personal privacy, the head of a public body must consider all the relevant circumstances, including whether

(a) the disclosure is desirable for the purpose of subjecting the activities of the Government of Alberta or a public body to public scrutiny

(b) the disclosure is likely to promote public health and safety or the protection of the environment,

(c) the personal information is relevant to a fair determination of the applicant's rights,

(d) the disclosure will assist in researching or validating the claims, disputes or grievances of aboriginal people,

(e) the third party will be exposed unfairly to financial or other harm,

(f) the personal information has been supplied in confidence,

(g) the personal information is likely to be inaccurate or unreliable,

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

(i) the personal information was originally provided by the applicant.

[para 15] Section 17 does not say that a public body is never allowed to disclose third party personal information. It is only when the disclosure of personal information would be an unreasonable invasion of a third party's personal privacy that a public body must refuse to disclose the information to an applicant under section 17(1). Section 17(2) (not reproduced) establishes that disclosing certain kinds of personal information is not an unreasonable invasion of personal privacy.

[para 16] When the specific types of personal information set out in section 17(4) are involved, disclosure is presumed to be an unreasonable invasion of a third party's personal privacy. To determine whether disclosure of personal information would be an unreasonable invasion of the personal privacy of a third party, a public body must consider and weigh all relevant circumstances under section 17(5), (unless section 17(3), which is restricted in its application, applies). Section 17(5) is not an exhaustive list and any other relevant circumstances must be considered.

[para 17] The Public Body applied section 17 to withhold personally identifying information of third parties in a police file. It is presumptively an invasion of personal privacy to disclose this information by operation of section 17(4)(b). From my review of the Public Body's application of section 17, I agree that disclosure of the information it severed would serve to identify individual third parties to the Applicant, with the exception of police member and Crown prosecutor cell phone numbers and direct lines, which I will discuss below. I also agree that there are no provisions of section 17(5) that weigh in favor of disclosure in this case. As a result, the presumption created by section 17(4)(b) and (g) is not rebutted.

[para 18] For the reasons above, I confirm the Public Body's application of section 17.

ISSUE C: Did the Public Body properly apply section 20(1) of the Act (disclosure harmful to law enforcement) to the information in the records?

[para 19] The Public Body applied sections 20(1)(g) and (m) to withhold information from the Applicant. It notes in its submissions:

> The Redactions made under sections 20(1)(g) and (m) of the FOIPP Act regard direct references to prosecutorial discretion and sensitive CPS communications system information. The Redactions therefore meet the requirements for section 20(1), and therefore the CPS may withhold such information.

[para 20] Section 20 states, in part:

> *20(1) The head of a public body may refuse to disclose information to an applicant if the disclosure could reasonably be expected to*
>
> > *(g) reveal any information relating to or used in the exercise of prosecutorial discretion,*
> >
> > *[…]*
> >
> > *(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system […]*
>
> *[…]*
>
> *(6) After a police investigation is completed, the head of a public body may disclose under this section the reasons for a decision not to prosecute*
>
> > *(a) to a person who knew of and was significantly interested in the investigation, including a victim or a relative or friend of a victim, or*
> >
> > *(b) to any other member of the public, if the fact of the investigation was made public.*

[para 21] I will first consider the Public Body's application of section 20(1)(g).

Section 20(1)(g)

[para 22] "Prosecutorial discretion" refers to a Crown prosecutor's power to bring, manage and terminate prosecutions. Decisions to bring, manage, or terminate prosecutions are exercises of prosecutorial discretion. Recorded information that reveals information relating to, or used in making decisions to bring, manage, or terminate prosecutions falls within the terms of section 20(1)(g).

[para 23] From my review of the information to which the Public Body applied section 20(1)(g), I agree that it reveals information regarding a Crown prosecutor's decision to bring, manage, or terminate a prosecution. I find that the information is subject to section 20(1)(g).

[para 24] Section 20(1)(g) is a discretionary exception – the head of a public body may withhold information falling within its terms from an applicant, but the head may also disclose the information. It is not enough that a public body demonstrate that recorded information falls within the terms of a discretionary provision, such as section 20(1)(g); the public body must also demonstrate that it exercised its discretion appropriately when it decided to withhold the information.

[para 25] In *Hearings Before Administrative Tribunals*, 2nd Edition[1], McCauley and Sprague describe how discretion is to be exercised when a statute confers discretion to make a decision. They state:

> When Parliament [or the Legislature] gives a decision-maker the discretion to make a decision, it expects the decision maker to make each decision on the basis of the circumstances in each individual case.
>
> If the Legislature [or Parliament] did not want this to be so it would not have granted the decision-maker discretion in the first place. It would have set out the circumstances and the thing to be done or authorized that those specifications be set out in regulation. The fact that Parliament granted the power in terms of a grant of discretion means that Parliament wanted the discretion to be exercised on a case-by-case basis.
>
> The underlying purpose in granting a decision-maker discretion is to guarantee flexibility and responsiveness in administrative decision-making. The decision-maker cannot frustrate this purpose by choosing to exercise that power on some other basis that the decision-maker feels is more efficient, effective or expeditious. The decision-maker must take its power as it gets it. The decision-maker will err if, rather than considering the […] decision on a case by case basis, it simply applies or follows earlier developed procedure or policy without considering whether that policy is appropriate to the particular case. This is known as fettering discretion.
>
> Having to decide a matter on a case-by-case basis means that the decision-maker must apply his or her mind to each matter, and all the components of that matter, and decide each of those components on the basis of their merit in those circumstances. This means that the decision-maker

[1] Robert W. McCauley and James L.H. Sprague, *Hearings Before Administrative Tribunals* 2nd Edition (Toronto: Thomson Canada Ltd. 2002) pp. 5B-15 – 5B-16

> must keep an open-mind on all aspects of the matter – procedural just as much as substantive – and decide what to do with the merits of each case.

[para 26] In *Ontario (Public Safety and Security) v. Criminal Lawyers' Association*, 2010 SCC 23, the Supreme Court of Canada explained the process for applying discretionary exceptions in freedom of information legislation and the considerations that are involved. The Court illustrated how discretion is to be exercised by discussing the discretionary exception in relation to law enforcement:

> In making the decision, the first step the head must take is to determine whether disclosure could reasonably be expected to interfere with a law enforcement matter. If the determination is that it may, the second step is to decide whether, having regard to the significance of that risk and other relevant interests, disclosure should be made or refused. These determinations necessarily involve consideration of the public interest in open government, public debate and the proper functioning of government institutions. A finding at the first stage that disclosure may interfere with law enforcement is implicitly a finding that the public interest in law enforcement may trump public and private interests in disclosure. At the second stage, the head must weigh the public and private interests in disclosure and non-disclosure, and exercise his or her discretion accordingly.

[para 27] While the foregoing case was decided in relation to the law enforcement provisions in Ontario's legislation, it is clear from paragraphs 45 and 46 of this decision that its application extends beyond law enforcement provisions to the application of discretionary provisions in general and to the discretionary provisions in freedom of information legislation in particular. Section 20(1)(g) of Alberta's FOIP Act is an example of a discretionary exception.

[para 28] Discretion must be exercised on a case by case basis. After determining that section 20(1)(g) applies, the head of a public body must then consider and weigh all relevant factors, including relevant public and private interests weighing in favor of disclosure or nondisclosure, in making the decision to sever information under this provision or to disclose it.

[para 29] The Public Body argues:

> In considering whether to withhold the redacted information, the CPS considered that the Applicant has a general right of access to the records in the custody or under the control of CPS, particularly with respect to personal information about him, and that such access is important to allow him to request corrections to such personal information. However, because the Redactions are in place to prevent the disclosure of prosecutorial discretion or sensitive communication systems information, which disclosure would harm law enforcement, and do not regard personal information about the Applicant, the CPS properly exercised its discretion to invoke section 20(1) as the harm outweighed the benefit.

From the foregoing, I understand that the Public Body took into consideration the purpose of section 20(1)(g) when it exercised its discretion to withhold information from the Applicant. In its view, there were no other relevant considerations. Nevertheless, I believe that there are other relevant factors that should be taken into consideration in making the decision to withhold information under section 20(1)(g).

[para 30] Section 20(6) of the FOIP Act authorizes the head of a public body to disclose information subject to section 20(1)(g) to a victim at the conclusion of an investigation, if a decision not to prosecute has been made. This provision recognizes the public interest in informing victims of the reasons for a Crown prosecutor's decision not to proceed, as well as a victim's private interests in that decision. From the information I have been given regarding the Applicant's criminal complaint, I conclude that the circumstances contemplated by section 20(6) may be met and could therefore weigh in favor of disclosure. The Public Body did not address section 20(6) in its submissions and so it is unclear whether it considered it.

[para 31] Another potential factor that the Public Body has not addressed in its discussion of its exercise of discretion is the fact that the statements to which it applied section 20(1)(g) indicate that the Crown prosecutor provided their substance to the Applicant. That the Crown prosecutor exercised discretion to provide the reasons in the records to the Applicant is a relevant factor weighing in favor of disclosure.

[para 32] The Public Body's decision to sever information under section 20(1)(g) considers primarily the purpose of the provision – to protect against the potential harm of disclosing information revealing a Crown prosecutor's reasons for exercising discretion in a particular way. However, section 20(6) establishes that there are circumstances in which the benefits of disclosure may outweigh the harm. Moreover, a Crown prosecutor has discretion, regardless of the FOIP Act, to disclose information about prosecutorial decisions, and it appears that the Crown prosecutor considered it appropriate to disclose information about the Crown's reasons to the Applicant. As a result, it is unclear what benefit would be served by withholding the information to which the Public Body applied section 20(1)(g), given that the information is a record of what the Crown prosecutor communicated to the Applicant at an earlier date.

[para 33] As the Public Body did not consider the application of section 20(6) or the fact that the information was provided to the Applicant originally, and these are relevant factors, I must direct the Public Body to make a new decision as to whether it will provide the records to which it applied section 20(1)(g) to the Applicant. There may be other relevant factors that weigh for or against disclosure that the Public Body did not take into consideration when it exercised its discretion initially or did not raise in its submissions. If so, the Public Body is not precluded from considering these factors in its new exercise of discretion.

Section 20(1)(m)

[para 34] As noted above, the Public Body withheld cell phone numbers and direct line numbers of police members and Crown prosecutors under sections 17 and 20(1)(m). It also severed the address of the Public Body's spam quarantine storage under section 20(1)(m).

[para 35] The Public Body's submissions regarding its application of section 20(1) are the following:

> The Redactions made under sections 20(1)(g) and (m) of the FOIPP Act regard direct references to prosecutorial discretion and sensitive CPS communications system information. The Redactions therefore meet the requirements for section 20(1), and therefore the CPS may withhold such information. All Redactions were proper.

Cell phone numbers and direct lines

[para 36] Public Bodies often assign direct lines and cell phone numbers to employees for specific types of work related calls, and another number, such as a main switchboard number, for calls from members of the public. For example, an employee may be given a direct line or cell phone number that other employees of the public body or senior officials may use to contact the employee. The general public does not have access to this number, but must contact the employee through a general switchboard system. In this way, the Public Body is able to ensure that calls are directed to the appropriate employees for response and that the employee does not have to field calls that are unrelated to the employee's work duties or that are inappropriate given those duties.

[para 37] Restricting access to employee direct lines and cell phone numbers serves a number of organizational purposes. If the employee has a decision making or adjudicative function, it prevents an interested party from communicating directly with the employee without other parties being present. Such calls may undermine the appearance of fairness of the adjudicative process, and are avoided for that reason. Similarly, if an employee is an investigator, such as a police officer, direct calls from witnesses or interested parties may interfere with an investigation. The evidence of witnesses, including police witnesses, may be given less weight at trial if the witnesses have discussed a case, or appear to have discussed a case, prior to giving testimony.

[para 38] If an employee has a high profile position, the direct line or cell phone number may receive so many calls as to become a nuisance if the number were to become public. In other cases, access to an employee's direct line or cell phone number may be restricted in order to protect the employee from harassing phone calls related to the employee's work or function. By having an employee's calls from the general public directed to a switchboard, a public body may screen phone calls before directing them to a particular employee's cell phone or direct line to ensure that the appropriate phone calls are referred to the correct employee, and to mitigate the risk of the outcomes I have listed.

[para 39] When I review the numbers severed by the Public Body, I am not convinced that section 17 is engaged. I say this because there does not appear to be a personal dimension to the numbers. They are included in emails to inform recipients (who are members of the Public Body or the Minister of Justice and Solicitor General) how to contact the employee to discuss work-related matters in the employee's capacity as a representative of the Public Body or Alberta Justice and Solicitor General.

[para 40] I note that the Public Body did not sever a police officer's phone number from his business card or email address from his communications, but severed the cell

phone number from the police officer's emails. The phone number on the business card is also business contact information; however, the Public Body presumably considered there to be little or no personal privacy at stake in giving out the number. At the same time, there is no difference between the two numbers from the perspective of personal privacy. Both are the business contact information of police officers; only one number is intended by the Public Body to be given to the general public and the other to police officers and to Crown prosecutors for work purposes. Both numbers could be the police officer's personal information, if it were accompanied by other information about the police officer as an identifiable individual. However, in the absence of such information, the business card and the cell phone number in emails communicate only that the numbers they contain are for the recipient to call the police officer to discuss police matters.

[para 41] I believe that the Public Body has decided not to provide the cell phone numbers and direct line numbers because providing the number could possibly result in the police officer receiving phone calls that could interfere with the police officer's ability to investigate files. It may also be concerned that by making the direct line or cell phone number available to the public by disclosing it through an access request, the phone number may receive harassing phone calls from members of the public.

[para 42] In Order F2020-13, which also involved the Public Body, the Director of Adjudication accepted that disclosing cell phone numbers could result in the harms contemplated by section 20(1)(m). She said:

> In this case, the CPS argues that the harms test set out for section 20(1) of the Act (see, e.g., in Order F2010-008 is met by the disclosure of police cell phone numbers because members of the public who are involved in criminal activities, such as dangerous offenders and gang members, could use the information to contact retired or off-duty officers to threaten or harass them. Such factors were not put forward or considered in Order F2010-008. I accept that this could be a possible result of public access to these numbers, and that the provision applies. I uphold the redaction of the cell phone number on this page, including its exercise of discretion.

[para 43] 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 44] As I noted in Order F2021-08, section 20 is a provision containing exceptions in relation to law enforcement. I said:

> Law enforcement is defined in section 1(h) of the FOIP Act in the following terms:
>
> *1(h) "law enforcement" means*
>
> *(i) policing, including criminal intelligence operations,*
>
> *(ii) a police, security or administrative investigation, including the complaint giving rise to the investigation, that leads or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the investigation or by another body to which the results of the investigation are referred, or*
>
> *(iii) proceedings that lead or could lead to a penalty or sanction, including a penalty or sanction imposed by the body conducting the proceedings or by another body to which the results of the proceedings are referred [...]*
>
> I was unable to identify information in the records that would interfere with law enforcement techniques, as defined above, or to systems used in law enforcement. The Public Body adopted a strategy developed and recommended by its Behavioral Science Unit to ensure the safety of its employees. Strategies of this nature are not unique to public bodies involved in law enforcement and may be adopted by all public bodies with responsibilities to protect the safety and physical and mental wellbeing of employees. A procedure or strategy is not a "law enforcement technique" simply because a public body that is involved in law enforcement uses it. Rather, as required by section 1(h), the technique must be used in an investigation, proceedings, or policing operations, before it will be considered a law enforcement technique falling within the terms of section 20. I am unable to find that the recommendations of the Behavioral Sciences Unit before me fall within these categories.

The concern that disclosure of a cell phone or direct line may expose an employee to harassment or unwanted calls is not unique to law enforcement. Public bodies not involved in law enforcement may also need to withhold cell phone numbers or direct line numbers from applicants or the public to ensure that employees are not contacted inappropriately.

[para 45] Although I do not agree with the Public Body's application of section 17 and 20(1)(m) to cell phone numbers and direct lines of police officers and Crown prosecutors, I believe that there is an exception in the FOIP Act that enables public bodies -- not only those involved in law enforcement -- to sever cell phone numbers and direct lines from records for the reasons I have discussed above: the concern that making the number public will render it unusable because of the likelihood that it will receive too many calls for the employee to reasonably answer, or be used by individuals who should not contact an employee directly, due to the nature of the employee's employment. If it can be anticipated that once a cell phone or direct line is made public, the public body will likely have to assign a new number, then section 25 of the FOIP Act applies to the number.

[para 46] 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:*
>
> *[…]*
>
> *(c) information the disclosure of which could reasonably be expected to*
>
> *(i) result in financial loss to,*
>
> *[…]*
>
> *the Government of Alberta or a public body[…]*

[para 47] Telephone service providers charge fees for providing cell phone and direct lines to employees and to change the numbers. A public body may also have to change internal directories and business cards to accommodate the change, which also involves spending public money. Section 25 will apply when there is a reasonable likelihood that a public body may have to change an unlisted cell phone or direct line if the number is disclosed.

[para 48] There will be occasions when an employer-provided unlisted cell phone or direct line number is personal information within section 17, such as when the number is accompanied by other information about the employee as an identifiable individual. There will also be situations, as discussed by the Adjudicator in Order F2019-09, where section 18 may apply to the numbers, as in the situation where it could reasonably be expected that an employee would be subjected to mental or physical harm if a direct line or cell phone number were given to an applicant and / or made public. In cases where a police matter is ongoing and direct contact with the investigator by cell phone or direct line could be harmful to the investigation, section 20(1)(a) may be engaged.

[para 49] Section 25 will apply to the telephone numbers assigned to a public body's employee if it can reasonably be expected that the Public Body will need to change the employee's telephone number once it has been provided to an applicant / made public through an access request. Evidence as to the reasons why a public body restricts access to the number, how it treats the employee's calls, the public body's organizational structure and purpose, and the employee's work duties, will be necessary to establish the application of section 25.

[para 50] From the records at issue, I understand that the police officers in this case do not provide cell phone numbers to witnesses or complainants to contact them directly regarding active cases, but use either email or the numbers on their business cards. In

this way, the Public Body is able to manage, to a certain extent, the kinds of business related calls officers receive, and that they are appropriately documented, and to ensure that police officers do not receive inappropriate calls that could compromise the integrity of investigations, among other kinds of inappropriate calls.

[para 51] If the Public Body were to release the cell phone numbers or direct lines to applicants, it would have no ability to control further dissemination of the numbers. The phone number could be used by any member of the public, including the Applicant, to contact police officers and Crown prosecutor whose numbers are contained in the records, in addition to the Applicant. If so, then it is reasonable to expect that both the Public Body and Alberta Justice and Solicitor General would have to assign new unlisted cell phone and direct line numbers to their employees if they are disclosed.

[para 52] It is unclear that the Applicant has any interest in obtaining the cell phone or direct line numbers, as he does not refer to these in his requests for review or inquiry and did not make submissions regarding them. It is unclear from his access request whether he intended to obtain such information when he made it.

[para 53] For all these reasons, I find that section 25(1) is engaged in relation to the cell phone and direct line numbers and that the interests in this case weigh in favor of withholding the numbers in this case.

Spam Account address

[para 54] The Public Body withheld the address for a police member's external spam quarantine folder under section 20(1)(m). It refers to this information in its submissions as "sensitive CPS communications system information". On the evidence before me, it is unclear that disclosure of an external spam quarantine folder address would have any effect on the security of the Public Body's email management systems, given that the police member's user name and password are not contained in the records at issue.

[para 55] At the same time, as noted above, the Applicant did not provide any submissions for the inquiry. It is unclear from his access request -- which is one for witness statements, reports, video and audio tape surveillance of a May 18, 2016 occurrence under CPS action #16211995 -- or his requests for review and inquiry, that the spam quarantine folder address is responsive to the access request, given that the spam quarantine folder address is unrelated to the investigation conducted by the Public Body that is the subject of the access request.

[para 56] While I am unable to support the Public Body's application of section 20(1)(m) on the evidence before me, I will not order the disclosure of the information, given that it is nonresponsive to the access request.

ISSUE D: Did the Public Body properly apply section 24(1) of the Act (advice from officials) to the information in the records?

[para 57] The Public Body severed a portion of an email between police officers and instructions for handling "Crime Stoppers" tips under section 24(1)(b). Section 24 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 […]*
>
> *(2) This section does not apply to information that*
>
> *[…]*
>
> > *(f) is an instruction or guideline issued to the officers or employees of a public body[…]*
>
> *[…]*

[para 58] The Public Body argues that section 24(1)(b) applies to the information it severed and characterizes the information as consultations or deliberations. I do not agree with this characterization. In my view, the information may be more properly characterized as "instructions or guidelines" for the Public Body's employees. If information falls within the terms of section 24(2)(f), reproduced above, it cannot be withheld under section 24(1), although other exceptions in the FOIP Act may apply to it.

[para 59] Although I do not agree with the Public Body's application of section 24(1)(b), I do not intend to order disclosure of the information for the reason that the Applicant did not request the severed information.

[para 60] The Applicant requested:

> Any and all information, including but not limited to witness statements, reports, video and audio tape surveillance of a May 18, 2016 occurrence under CPS action #16211995. I specifically require a copy of the 7-11 video.

[para 61] The access request is for information such as witness statements, reports, video and audio tape surveillance in case file 16211995. The information severed by the Public Body under section 24(1)(b) is not part of the investigation and is not a witness statement, report, video or audiotape surveillance, or similar information relating to CPS action file #16211995. The information I find to be directions to staff are not in relation to this file. For this reason, I find that this information is nonresponsive.

IV. ORDER

[para 62] I make this Order under section 72 of the Act.

[para 63] I confirm the decisions of the Public Body to withhold information from the Applicant, with the exception of the information to which it applied section 20(1)(g).

[para 64] I direct the Public Body to reconsider its exercise of discretion to withhold the information to which it applied section 20(1)(g), as discussed in the order, above.

[para 65] I order the Public Body to inform me within 50 days of receiving this order that it has complied with it.

_____

Teresa Cunningham
Adjudicator