ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

ORDER F2024-33

November 4, 2024

CALGARY POLICE SERVICE

Case File Number 015795

Office URL: www.oipc.ab.ca

Summary: The Applicant requested his personal information from the Calgary Police Service (the Public Body) on three occasions. In the most recent request, the Public Body limited its search to information that had not been the subject of previous searches. The Public Body located some records, but severed information from them under sections 17 (disclosure harmful to personal privacy) and 20 (disclosure harmful to law enforcement).

The Applicant requested review by the Commissioner of the Public Body's most recent response to his access request, but not his previous requests.

The Adjudicator found that the Public Body had met the duty to assist under section 10(1) by conducting a reasonable search with the exception of records documenting the Applicant's complaints. The Public Body explained that it had not previously searched for records regarding his complaints as its FOIP unit had not had access to a database in which complaints were stored. The Adjudicator ordered the Public Body to include the complaints it had located in its response to the Applicant.

The Adjudicator determined that section 20 of the FOIP Act did not apply to the information severed by the Public Body under this provision. She ordered the Public Body to give the Applicant access to this information. The Adjudicator confirmed that section 17 required the Public Body to sever the personal information of individuals other than the Applicant where it appeared in the records.

Statutes Cited: AB: *Freedom of Information and Protection of Privacy Act* R.S.A. 2000, c. F-25, ss 1, 9, 10, 17, 18, 20, 66, 72

Authorities Cited: AB: Order F2007-029

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

I. BACKGROUND

[para 1] The Applicant wrote a letter to the Chief of the Calgary Police Service (the Public Body) in which he complained that the Public Body had not properly investigated his complaints regarding police conduct. He also complained about the way the Public Body responded to access requests in the past. He concluded by making a new request for records he had previously requested but the Public Body had not produced, but also requested "all other reports and records in possession of or accessible by, the CPS relating to me."

[para 2] In an October 1, 2019 email to the Calgary Police Service, the Applicant confirmed that he was requesting the following under the *Freedom of Information and Protection of Privacy Act* (the FOIP Act):

> I want everything the CPS has access to or in its possession relating to me from 2011 to date – dispatch recordings, files, reports, digital taser records, body cam footage, any other video/audio recordings, CPIC records, alleged reports I am a freeman on the land – everything.

[para 3] The Public Body responded to the Applicant in an email dated October 25, 2019. The Public Body noted that it had responded to access requests for the same information previously and that the Applicant had not requested review by the Commissioner of its responses to those access requests. The Public Body provided access to records it located regarding an incident that took place in 2018 for which it had not previously searched, as the records had been created in the time following the Applicant's previous requests.

[para 4] The Applicant requested review of the Public Body's October 25, 2019 response.

[para 5] The Commissioner agreed to conduct an inquiry regarding the Public Body's October 25, 2019 response, but not its past responses to access requests.

II. ISSUES

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

Issue B: Does section 20(1) (disclosure harmful to law enforcement) authorize the Public Body to withhold information from the Applicant?

Issue C: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) require the Public Body to withhold information from the Applicant?

III. DISCUSSION OF ISSUES

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

[para 6] Section 10(1) of the FOIP Act creates a duty to assist applicants. It 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.*

Past orders of this office have interpreted the duty to assist as including the duty to conduct a reasonable search for responsive records.

[para 7] 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) [now10(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.

[para 8] From the foregoing, I understand that the duty to assist also has an informational component. A public body must conduct a reasonable search and inform the applicant of what has been done.

[para 9] The Public Body explained the search it conducted for responsive records:

> In reviewing the file, I can confirm the following as it relates to the adequacy of search in question:
>
> This file was assigned to an experienced Disclosure Analyst, who had been with the Access and Privacy Section of the Calgary Police Service in the role of Disclosure Analyst for over 9 Years at the time.
>
> As the Access Request referenced prior requests the Disclosure Analyst went back and reviewed those requests prior to commencing the search for records. Where the information requested was the same as for the prior request the Disclosure Analyst relied on the earlier search, but they did conduct a new search for records that may have been created since the earlier request (see order 99-021). In this case, due to the Applicant's allegations of incomplete records the Disclosure Analyst also checked to make sure there were no additional records relating to the earlier request that had not been previously disclosed.
>
> The Disclosure Analyst commenced the search by searching the Applicant's name in Sentry. The Sentry database contains every report that the police have created so by searching by the Applicant's name, every case file is returned as a hit. The Disclosure Analyst then went through the hits to determine which were responsive to the request. There would not be any repository of records other than Sentry that would have to be searched to locate police Occurrence Reports relating to an individual. Results in Sentry can be narrowed by date of birth or middle name to exclude results that relate to another individual with the same name. In this case, the Disclosure Analyst started with the broad search, not limited by DOB or middle name and then excluded non-responsive records. In addition, the reviewing of these records would identify other areas of the Service that may need to be searched to obtain further records.
>
> The Disclosure Analyst then retrieved the records that had not previously been provided. To ensure completeness of search the Disclosure Analyst then conducted a further search of the INET system for any calls to the Applicant's address. This INET system is a database of CAD (Computer Aided Dispatch) calls and may contain calls for which no Occurrence Report was created. Based on that search, the Disclosure Analyst learned that the Applicant may also have been staying at an alternate address and queried that address.
>
> The Disclosure Analyst then conducted a search of the CPS Palantir system to try and locate any additional records. Palantir is an information and data aggregator which permits a Disclosure Analyst to ensure that searches of the individual databases have retrieved all responsive records. The Palantir Search did not identify any additional records thereby satisfying the Disclosure Analyst that she had located all responsive records.
>
> Sometimes an applicant thinks records should exist when they simply do not. Body Worn Camera (BWC) is an example. The Applicant requested BWC in this new request. The Calgary Police Service currently has BWC but we did not in 2017. People just assume because we have it now, we always have had it which is not the case. Based on the thoroughness of the Disclosure Applicant's search in 2017 and the subsequent search on file 19-P-3131 the Public Body is of the belief no further records exists. There are no repositories of records where records could be that were not searched, and the search terms utilized were broad and would have located responsive records.

[para 10] The Public Body has explained how it conducted the search, who conducted it, where it located records, what it found, and why it believes no additional records exist.

[para 11] The Applicant argues:

> Attached at pages 1-2 is the 2017-05-18 email from then-CPS FOIP Disclosure Analyst […], informing the applicant that nine out of ten categories of requested materials were not being provided to me under section 4(1)(k) of the Act (the request is attached at pages 3-4). She alleged they were ineligible for release until one full year passed from the staying of various criminal proceedings and invited me to reapply, which I did in 2019. On October 25, 2019, the same analyst told me that she would not provide any previously requested materials that were not provided and that I should have applied to OIPC for review. This is contrary to the purpose in provisions of the Act. The public body's 2017 response reflects the intentions of section 9 of the Act, essentially promising that this was a "continuing request", which the analyst did not honour. Section 9 of the Act provides: Continuing request 9(1) The applicant may indicate in a request that the request, if granted, continues to have effect for a specified period of up to 2 years. (2) The head of a public body granting a request that continues to have effect for a specified period must provide to the applicant (a) a schedule showing dates in the specified period on which the request will be deemed to have been received and explaining why those dates were chosen, and (b) a statement that the applicant may ask the Commissioner to review the schedule. (3) This Act applies to a request that continues to have effect for a specified period as if a new request were made on each of the dates shown in the schedule. No specific time limitation for re-applying was given and the only condition was that one year must elapse from the time of the stays of proceedings to reapplying. Again, it is irrelevant how many times an application is submitted; the applicant is entitled to records he never received that are not restricted by any other provision – which they are not.

The Applicant is not concerned with the information the Public Body located and provided to him in previous searches, but information that he believes ought to exist, but was not located or provided. The Applicant argues that the Public Body is not entitled to rely on its responses to past access requests, even though the Applicant did not request review of those responses. The Applicant's position is that his request was a continuing request within the terms of section 9 and continued to have effect for up to two years.

[para 12] Section 66 of the FOIP Act imposes time limits on the ability to request review. It states, in part:

> *66(1) To ask for a review under this Division, a written request must be delivered to the Commissioner.*
>
> *(2) A request for a review of a decision of the head of a public body must be delivered to the Commissioner*
>
> *(a) if the request is pursuant to section 65(1), (3) or (4), within*
>
> *(i) 60 days after the person asking for the review is notified of the decision, or*
>
> *(ii) any longer period allowed by the Commissioner,*
>
> *or*

(b) if the request is pursuant to section 65(2), within 20 days after the person asking for the review is notified of the decision.

[para 13] The Commissioner will review a public body's response to an access request provided the applicant requests review of the response within 60 days of receiving it or the Commissioner allows a longer period. The Applicant requested review of the Public Body's response of October 25, 2019 but did not request an extension of the time for requesting review in relation to the previous responses. He did not request review of the previous responses.

[para 14] The Applicant argues that he made a "continuing request" for records within the terms of section 9 of the FOIP Act. He reasons that this means the Public Body has an ongoing duty to produce records he expected to receive in response to past access requests and that this duty is reviewable in this inquiry. Section 9 of the FOIP Act states:

9(1) The applicant may indicate in a request that the request, if granted, continues to have effect for a specified period of up to 2 years.

(2) The head of a public body granting a request that continues to have effect for a specified period must provide to the applicant

(a) a schedule showing dates in the specified period on which the request will be deemed to have been received and explaining why those dates were chosen, and

(b) a statement that the applicant may ask the Commissioner to review the schedule.

(3) This Act applies to a request that continues to have effect for a specified period as if a new request were made on each of the dates shown in the schedule.

[para 15] Section 9 applies in the situation where an applicant requests that the access request be in effect for a 2-year period. Section 9 typically encompasses the situation where the records the applicant has requested will be created after the access request is made. As indicated by the phrase, "if granted" in section 9, the head of a public body must grant the request to hold an access request open for a 2-year period before this provision will apply. In the current case, there is no evidence that the Applicant requested that his previous access requests be kept open for a 2-year period or that the head of the public body granted any such request. As a result, I find that section 9 has no bearing on the issues in this inquiry.

[para 16] The Applicant did not request review of the Public Body's responses to his past access requests under section 66 of the FOIP Act. For this reason, those responses are not before me. The only response I may review is the Public Body's response of October 25, 2019.

[para 17] The Public Body has explained the steps it took to locate responsive records, which included looking for any records that had not been the subject of searches when it responded to previous access requests. It also states that it checked to make sure that no records had been omitted in its responses to previous access requests, as the Applicant had complained about missing records.

[para 18] With one exception, I accept that the Public Body conducted a reasonable search for responsive records even though it did not conduct searches for records that were the subject of past searches.

[para 19] With regard to the exception, I note that the Public Body states:

> Item f: records relating to the report at page 12 – the second InfoPost Summary report, for example the complaints to PSS and outcomes referred to, history of fleeing traffic stops etc. We conducted a search in the PSS tracking system and located 5 PSS complaints from this Applicant. Three of these complaints were made prior to the August 2019 access request. We have not pulled these records and if the Applicant would like them, they can open a new request and we will process it. The former Analyst would not have reviewed records from the PSS tracking system as the Access & Privacy Section did not have access at the time and nor was it standard practice to locate records there unless specially directed to by the Applicant. Since the time of this request, the Section now has access, and it is now standard practice to review records from Professional Standards if the Applicant requests everything.

[para 20] It is unclear why the Public Body believes the Applicant must make a new request for the records it located from the PSS tracking system. The Applicant's access request is for information in the Public Body's custody or control relating to him. The Public Body's description of these records indicates that their content relates to the Applicant. As a result, the records appear to be responsive. The Public Body also indicates that these records were not the subject of a previous search. I find that the Public Body is required to include these records in its response to the Applicant.

[para 21] To conclude, I find that the Public Body conducted a reasonable search for responsive records and met its duties to the Applicant as required by section 10 of the FOIP Act, but for the records located in its PSS tracking system. With regard to the records located in the PSS tracking system that preexisted his access request I must order the Public Body to include them in its response to the Applicant as they are responsive to the Applicant's access request and the Public Body has not yet conducted a search for them. The Public Body will not be precluded from applying any exceptions to disclosure that may apply.

Issue B: Does section 20(1) (disclosure harmful to law enforcement) authorize the Public Body to withhold information from the Applicant?

[para 22] The Public Body applied sections 20(1)(c) and (m) to some information in the records. Section 20 of the FOIP Act authorizes the head of a public body to withhold information from an applicant where disclosure could result in harm to law enforcement. It 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

[…]

(c) harm the effectiveness of investigative techniques and procedures currently used, or likely to be used, in law enforcement,

[…]

(m) harm the security of any property or system, including a building, a vehicle, a computer system or a communications system […]

[…]

[para 23] Section 20(1)(c) applies when an investigative technique or procedure used in law enforcement could reasonably be expected to become less effective if information is disclosed. Section 20(1)(m) applies when the security of property or system, such as a building, vehicle, or computer system, could be compromised or harmed by disclosure.

[para 24] In *Ontario (Community Safety and Correctional Services) v. Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 (CanLII), (*Ontario (Community and Correctional Services))* 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* adopted the "reasonable expectation of probable harm" formulation and it should be used wherever the "could reasonably be expected to" language is used in access to information statutes. As the Court in *Merck Frosst* emphasized, the statute tries to mark out a middle ground between that which is probable and that which is merely possible. An institution must provide evidence "well beyond" or "considerably above" a mere possibility of harm in order to reach that middle ground: paras. 197 and 199. This inquiry of course is contextual and how much evidence and the quality of evidence needed to meet this standard will ultimately depend on the nature of the issue and "inherent probabilities or improbabilities or the seriousness of the allegations or consequences": *Merck Frosst*, at para. 94, citing *F.H. v. McDougall*, 2008 SCC 53 (CanLII), [2008] 3 S.C.R. 41, at para. 40.

[para 25] Section 20 employs the phrase "could reasonably be expected to". As discussed in *Ontario (Community and Correctional Services) (supra)* when this phrase is used, it refers to a reasonable expectation of probable harm. Section 20 of the FOIP Act uses this same phrase. Accordingly, the onus is on the Public Body to establish that it has a reasonable expectation that disclosure would result in harms that are probable and not merely speculative. In order to do so, it must explain why it believes the harms it envisions could reasonably be expected to result from disclosure of the specific information.

[para 26] The Public Body provided *in camera* submissions in order to be able to discuss the content of the records and its reasons for applying section 20(1)(c) and (m) as it did.

[para 27] Having reviewed the Public Body's submissions, I am unable to find that either section 20(1)(c) or (m) applies to the information severed by the Public Body under these provisions. The Public Body envisions general harm if all information of the type it severed is disclosed, including information of other individuals. It does not explain its application with respect to the actual information it severed. The information severed by the Public Body does not reveal any information about the Public Body's systems, nor does it reveal information about techniques used in investigations. In addition, the Public Body does not explain how the disclosure could reasonably be expected to result in the harm contemplated by section 20(1)(c) or (m) as it has not explained how disclosure of the information it severed could reasonably be expected to harm its property or systems or investigative techniques.

[para 28] Some of the information the Public Body severed could be considered to be a part of a system of categorizing information; however, there is no evidence that the system itself would be harmed by disclosure. It is unclear that the information the Public Body severed under section 20 reveals anything regarding investigative techniques. If it is assumed that a system of characterizing subjects is an investigative technique, it is not

clear how the investigative technique will be less effective as a result of disclosure of the severed information.

[para 29] I have also considered whether section 18 (disclosure harmful to individual or public safety) of the FOIP Act could potentially apply, given that the Public Body's reasons for applying section 20 are addressed by section 18. Section 18 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.*
>
> *[...]*

The evidence before me is inadequate to establish that the Public Body has a reasonable expectation of probable harm to individual or public safety arising from disclosure of the information to which it applied section 20.

Issue C: Does section 17(1) of the Act (disclosure an unreasonable invasion of personal privacy) require the Public Body to withhold information from the Applicant?

[para 30] 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.

[para 31] Section 1(n) of the FOIP Act defines personal information. It states:

> *1 In this Act,*
>
> > *(n) "personal information" means recorded information about an identifiable individual, including*
> >
> > > *(i) the individual's name, home or business address or home or business telephone number,*
> > >
> > > *(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,*
> > >
> > > *(iii) the individual's age, sex, marital status or family status,*
> > >
> > > *(iv) an identifying number, symbol or other particular assigned to the individual,*

(v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

(vi) information about the individual's health and health care history, including information about a physical or mental disability,

(vii) information about the individual's educational, financial, employment or criminal history, including criminal records where a pardon has been given,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else;

[para 32] Information is "personal information" within the terms of the FOIP Act if it is recorded and is about an identifiable individual.

[para 33] Section 17 sets out the circumstances in which a public body may or must not disclose the personal information of a third party in response to an access request. It 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.

[…]

(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 34] 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 (such as the Applicant in this case) 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 35] 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 36] The Public Body applied section 17(1) to withhold information that would reveal the names and other personally identifying information of individuals other than the Applicant whose personal information is contained in the requested records. I find that this information falls within the terms of section 1(n) of the FOIP Act, cited above. Section 17(4)(b) and (g) apply to this personal information as the information is clearly part of a police file and contains the names of the individuals in the context of other personal information about them. The personal information is therefore subject to a presumption that it would be an unreasonable invasion of personal privacy to disclose it. I agree with the Public Body's application of section 17(1) as the presumption created by section 17(4)(b) and (g) is not rebutted.

[para 37] To conclude, I find that the Public Body is required to withhold the information it severed under section 17(1) from the Applicant.

IV. ORDER

[para 38] I make this Order under section 72 of the Act.

[para 39] I require the Public Body to withhold the information to which it applied section 17(1) of the FOIP Act from the Applicant.

[para 40] As I find the Public Body is not authorized or required to withhold the information to which it applied section 20 from the Applicant, I order it to give the Applicant access to this information.

[para 41] I order the Public Body to include the records it located in its PSS system in its response to the Applicant.

[para 42] 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