MANITOBA OMBUDSMAN

# FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT INVESTIGATION REPORT

The City of Winnipeg – Winnipeg Police Service

Refusal of Access

**CASE# MO-00294 (2021-2715)**
**Final Report with Recommendations**

Issue Date:
February 27, 2025

**Provisions considered:**
**FIPPA 7(2), 17(1), 17(2)(b), 17(2)(e), 17(3)(i), 24(a), 25(1)(a), 25(1)(e), 29.2(a) and 29.2(b)**

# SUMMARY

The complainant made two applications for access to the City of Winnipeg - Winnipeg Police Service (the WPS) for copies of written complaints and compliments submitted to the WPS Professional Standards Unit. The WPS refused access to the records in full on the basis that the information was the personal information of identifiable individuals. A complaint was made to our office relating to this access decision. We reviewed two samples of the responsive records.

We found that, while some records could not reasonably be severed, other records could reasonably be severed to give access to some information that was not subject to the exception. The Ombudsman recommends that the WPS issue a revised access decision granting access to the records in part.

# TABLE OF CONTENTS

# INTRODUCTION

The access to information system in Manitoba is designed to promote access as a rule not the exception. FIPPA allows the public the right of access to information held by public bodies with limited and specific exceptions.

Any severing of information from records must be reasonable and severing should be done to allow as much information as possible to be provided to the person requesting the information.

In general, the purpose of exceptions to access is to prevent some form of harm being caused by the release of the information. Sometimes that potential harm is readily apparent, such as with an unreasonable invasion of privacy caused by the unauthorized disclosure of an individual's personal health information.

Other times it is not readily apparent, and it is the responsibility of the public body citing the exception to show that the withheld information is the type described in the exception and that the decision to withhold the information is reasonable in the circumstances.

The purpose of an investigation by our office is to review the decision of the public body and determine whether it complied with the requirements of FIPPA and appropriately applied the exceptions to access, keeping in mind the overarching principle that access to information should be the default position in relation to information in the custody or the control of public bodies.

# BACKGROUND

On August 27, 2021, the complainant made access requests to the City of Winnipeg – Winnipeg Police Service (the WPS or the public body) for the following records:

- (WPS File: 21 08 673): Written compliments submitted to the Winnipeg Police Service's Professional Standards Unit, submitted either in person or electronically, by members of the public between Jan. 1, 2015 – Jan. 1, 2021. If possible, we'd like to see the compliments written in full spare information that may identify the complementor or the officer with the WPS.

- (WPS File: 21 08 674): Written complaints submitted to the Winnipeg Police Service's Professional Standards Unit, submitted either in person or electronically, by members of the public between Jan. 1, 2015 – Jan. 1, 2021. If possible, we'd like to see the complaints written in full spare information that may identify the complainant or the officer with the WPS.

The WPS responded on September 3, 2021, and refused access in full. The public body cited subsection 17(1) and clauses 17(2)(b), 17(2)(e) and 17(3)(i) of FIPPA as the basis for its decision. On October 20, 2021, a complaint was made to our office about this access decision.

## INVESTIGATION

As part of our investigation, our office asked the WPS to provide us with copies of the responsive records as well as representations about how it determined that the cited sections of FIPPA applied to the information within the records.

The WPS advised in its decision letter that it had reviewed a sample of the responsive records (one compliment and one complaint) and determined that severing the personal information of identifiable individuals was not possible.

Due to the number of responsive records, the WPS requested to provide our office with the sample of the responsive records that it reviewed, rather than all the responsive records. Our office agreed to an initial assessment of the responsive records in this manner.

On December 9, 2021, the public body provided a sample of the responsive records (five complaints and four compliments) along with an additional explanation for how the public body determined that the cited sections of FIPPA applied. The WPS also provided additional information about considerations that went into making this decision.

The WPS indicated that the records contained the personal information of both police officers and members of the public and that the information needed to be redacted to protect the privacy of both. The WPS also indicated that reasonable severing was not possible because once the personal information was redacted, nothing meaningful would remain.

The WPS noted that on its complaint and compliment forms it states, "Your information will be used to respond to you and to assure service quality." The WPS stated that, because of this statement, people would expect what they wrote to be kept explicitly confidential. The public body also noted that people who submit complaints are often intimidated by the process and are emotionally affected by their experiences.

The public body indicated it did not think it was appropriate to disclose the personal information of citizens without their consent and that it would also be inappropriate to request consent from these individuals given the circumstances. The WPS also indicated it would not want the potential for their information to be disclosed to deter citizens from making complaints against the WPS.

With regards to police officers named in the complaints and compliments, the WPS stated that there is a possibility that members could be identified by incident specifics, both internally by their colleagues and externally by the public. The WPS took the position that severing their names and badge numbers would not be sufficient to prevent the police officers from being identified.

The WPS also set out other considerations that affected its decision, unrelated to the application of section 17. The WPS indicated that some of the complaints involve ongoing investigations, and all complaints could be re-opened at any time if necessary.

The public body also indicated that there was a large number of records involved, and it was determined that an Estimate of Costs would not be issued as it would be unfair to the complainant to do so when they would only receive non-substantive information.

Lastly, the WPS considered it to be an unreasonable demand on its operations to review the files to determine which ones are open (under investigation) or may be re-opened.

Our office reviewed the sample of five complaints and four compliments provided by the WPS. There is no question that the complaints and compliments contain personal information of members of the public and of officers, which would be subject to mandatory exceptions to access under section 17 of FIPPA.

The only question is whether the records can reasonably be severed to give access to some information without releasing information that can be linked to identifiable individuals.

Based on our review of this sample of records, our office agreed with the WPS' assessment that severing the personal information of identifiable individuals in the records would mean that the complainant only received disconnected bits of information that would provide little value or context.

Our office contacted the complainant and discussed our review of the records. The complainant indicated that they recognized that some of the requested records would not be able to be severed. However, they asked our office to review another sample, to make sure that the sample was representative of the responsive records.

The complainant proposed that a further sample could be made up of all the complaints and compliments for a couple of months in two different years. Our office determined this was a reasonable approach. On July 20, 2022, we requested that the WPS provide us with additional records for review.

The WPS provided us with another eight complaints and one compliment on August 11, 2022. We reviewed these complaints and compliment and, unlike with the initial sample, determined that reasonable severing of some of the records in the second sample was possible. In fact, the copy of the records provided to our office was already severed with all the names of police officers and individuals removed.

While there was additional information, other than names, in the records that would likely need to be redacted under section 17, to avoid identifying the parties, it was our view that doing so would still leave meaningful information that could be disclosed after redaction.

Based on this review, our office contacted the complainant to explain our assessment that some records could be released with severing and to confirm that they were still interested in receiving the records, if some were released with severing and some were withheld in full.

We also explained to the complainant that if the public body issued a revised access decision, they should anticipate that some of the information in some records would be redacted and some records may still be redacted in full. The complainant indicated that they understood and still wished to proceed.

Our office then contacted the WPS on December 20, 2022, to provide our reasoning for why we felt some records could be released with severing and requested that they consider issuing a revised access decision and providing the complainant with redacted copies of the responsive records.

The WPS responded to our request on February 24, 2023. In its response the WPS indicated that it maintained that the records should be withheld in full, and raised several points, some of which were raised for the first time. The WPS also indicated that it had reassessed what records should be considered responsive to the requests for access.

Specifically, in relation to identifying the records responsive to the requests, the WPS indicated that, because the requests for access asked for records "submitted to the Winnipeg Police Service's Professional Standards Unit", it would exclude any complaints and compliments that were submitted to entities outside of the Professional Standards Unit (the PSU).

The WPS indicated that, because of this reassessment, some of the records of complaints submitted to our office for review were not actually responsive and should not form the basis for our analysis.

The WPS further indicated that it maintained that members of the public have an expectation that information they submit to the public body would be kept confidential and that this position was supported by the fact that the WPS has never routinely made such information public. The WPS also stated that if members of the public intended to make their complaints and compliments public, they could do so by sharing them directly with the media or on social media.

The WPS stated the view that FIPPA is ambiguous on how information related to the conduct of police officers (and associated compliments and complaints) should be handled. The WPS noted that this was different than legislation in other provinces, which they believe provides clear guidance on this topic. The WPS did not elaborate further on this point.

The WPS also cited three additional sections of FIPPA in support of its position that the information should not be disclosed, sections 24, 25 and 29.2. Specifically, the WPS cited clauses 25(1)(a), 25(1)(e), and subsections 24(a), 29.2(a) and 29.2(b).

Our office reviewed the information provided by the WPS, conducted additional research into this matter and had further discussions with the public body about its position. On May 2, 2023, our office sent a letter to the WPS fully setting out our analysis and views and again requested that the public body consider issuing a revised access decision and releasing the responsive records with reasonable severing of identifiable personal information.

We noted at this time that if the WPS intended to rely on additional exceptions to access, apart from section 17, it would be required to issue a revised access decision to the complainant stating this.

The WPS responded to our letter on July 31, 2023, and again indicated that its position was that the responsive records are being appropriately withheld in full under the cited sections of FIPPA and it would not be issuing a revised access decision.

The WPS also provided additional details in relation to how it determined that the records were not severable, and the applicability of the cited exceptions to access. The WPS also provided several documents in support of its position for our review.

# PRELIMINARY ISSUES

Before discussing the analysis of the relevant sections of FIPPA in the case, there are several preliminary issues that must be addressed, which were raised in the representations provided by the WPS.

## Records Responsive to the Request

In its representations, the WPS indicated that it had reconsidered which records were responsive to the access requests made by the complainant based on the wording of the access requests.

Specifically, the WPS determined that the responsive records should be limited to those submitted directly to the PSU by members of the public and should not include complaints or compliments that were sent to other entities within the WPS and the City of Winnipeg and then forwarded to the PSU.

We reviewed the samples of records provided to our office and it was evident based solely on the records themselves that all but one of the sample of complaints/compliments was sent to the PSU, if not by the member of the public directly, then by a public body employee after receiving it from a member of the public.

The sample records were either sent directly to the PSU through its online form or were forwarded to the PSU through email. In only one of the records was it unclear whether the PSU received a copy of the complaint/compliment.

Our office expects all public bodies to meaningfully interpret requests for access and to speak with the applicant to ensure that the public body's interpretation is consistent with what the applicant intended. This is part of the public body's duty to assist under FIPPA.

> ***Duty to assist applicant***
> ***9*** *The head of a public body shall make every reasonable effort to assist an applicant and to respond without delay, openly, accurately and completely.*

Because public bodies are the experts in their own records, they are in the best position to assist an applicant in ensuring that the records they request contain the information they are looking for. The duty to assist places a positive obligation on public bodies to take all reasonable efforts to help applicants and applies throughout the request process.

Requests for access should only be interpreted narrowly after speaking with the applicant to ensure that the proposed interpretation both accurately captures the records that the applicant wants and does not unreasonably exclude those that contain the information of interest to the applicant.

Discussion with the applicant can also help narrow or focus a request to prevent or limit the need for a fee estimate if there is a large number of records to be searched or provided.

However, once a public body has interpreted the request for access and issued an access decision, it is not reasonable to unilaterally re-interpret the meaning of the access request without first discussing this with the applicant. Doing so is not fair to the applicant, who is entitled to rely on the public body's original interpretation of the responsive records, particularly when it captured the applicant's intent. It would also not be consistent with the public body's duty to assist.

Based on this, despite the WPS' position that the scope of the requests should be reassessed, our office conducted its review based on the original access decision, which is based on the original interpretation of the requests for access, and the records already identified as responsive.

Specifically, we found that any complaints or compliments that were ultimately submitted to the PSU are responsive to the requests, regardless of who they were originally submitted to.

## The Application of Additional Exceptions to Access

If a public body determines, after making its initial access decision, that additional or different exceptions to access appropriately apply to the information contained in responsive records, then it must issue a revised access decision to the applicant before it is able to rely on those exceptions as the basis for its refusal of access. It is a fundamental matter of fairness that the applicant knows the basis and reasons for the decision.

Section 12 of FIPPA sets out what information a public body is required to provide to the applicant in response to a request for access. Specifically, subclause 12(1)(c)(ii) requires public bodies to inform applicants of the specific provisions on which the refusal of access is based.

> ***Contents of response***
> ***12(1)*** *In a response under section 11, the head of the public body shall inform the applicant*
>
> *(c) if access to the record or part of the record is refused,*
>
> *(ii) in the case of a record that exists and can be located, the reasons for the refusal and the specific provision of this Act on which the refusal is based,*

For a public body to meet its responsibilities under section 12 it must inform an applicant of all the relevant sections of FIPPA being relied upon and explain how the section applies to the information and how the public body made its decision. This requirement remains in effect even if a complaint is made or the public body subsequently determines that other sections of FIPPA apply to the information in replacement of, or in addition to, the previously cited exceptions.

Generally, if a public body references a new discretionary exception to our office in its representations and does not issue a revised access decision informing the complainant of this, as is the case here, our office does not consider whether the new discretionary exceptions to access apply to the responsive records.

Although the public body did not provide a revised access decision to the complainant, given the extent of the representations made by the public body, we felt it was important to address key considerations they raised about the application of sections 24, 25 and 29.2, including analysis about the application of these exceptions.

We will not be making findings as to whether those sections apply to specific information within the responsive records as the public body did not suggest specific information could be redacted under those sections, but rather made a general argument that those sections would apply to the responsive records.

However, we will be reviewing considerations related to the application of those exceptions, in general, in order to inform the public body and the complainant as to how our office would approach these sections if they form part of future access decisions we may review.

Our analysis in this case will examine the various requirements of FIPPA and how they apply to information in the records we reviewed in this case as well as the representations made to our office by the WPS.

## Ongoing Investigations/Potential for Re-opening Investigations

In its initial response to our office, the WPS indicated that one of the issues with providing access to the responsive records was the fact that, while some investigations into complaints are marked "closed" or "complete", these investigations can be re-opened as needed, such as if a pattern of behaviour becomes apparent at a later date.

Our office understands and recognizes the importance of protecting the integrity of an investigation while it is ongoing or during the appeal period once a decision has been made. However, natural justice and procedural fairness are core principles of both criminal and administrative law, which includes an individual's right to have their matters dealt with without delay.

It is well established in Canadian legislation and case law that investigations, court cases, and administrative processes must have a time limit. For example, FIPPA gives our office 2 years from the day we determine we have sufficient evidence to justify a prosecution to commence a prosecution under FIPPA.

The principles of natural justice and procedural fairness apply to both internal and external investigations conducted by public bodies, including the WPS. At some point, using a complaint as the basis for an investigation or as evidence in another investigation will no longer be reasonable or fair.

Conduct of police officers in the WPS is governed by the *Winnipeg Police Service Regulation By-Law*[1] (the By-Law), which states in its preamble:

> ***AND WHEREAS*** *the Winnipeg Police Association and the Winnipeg Police Senior Officers Association and the Winnipeg Police Service agree that a member of the Winnipeg Police Association or the Winnipeg Police Senior Officers Association who is the subject of a complaint will have the full protection of the rules of* ***natural justice*** *and the* ***principles of fairness*** *during the processing of the complaint;*
>
> *(emphasis added)*

The By-Law sets out the type of conduct that is considered appropriate for police officers and how defaults in conduct should be dealt with, including penalties. Sections 25, 29, 30, 32, 33, 34, 46, 50, 51, 54, 55, 57, 59, 67, and 69 all set out time limits for various stages of the investigation, review, discipline, and appeals related to defaults in police conduct. It is clear from the wording of the By-Law, that complaints against police officers will come to an end and cannot proceed in perpetuity.

The position taken by the WPS that it is impossible to know when and if an investigation will be re-opened is not supported by the requirements of the By-Law and the principles of natural justice and procedural fairness.

Additionally, if the WPS intends to deny access to information on this basis, then it would need to cite a relevant section of FIPPA and give reasons for how that section applies to the information and how it determined that redacting the information was an appropriate exercise of its discretion in the circumstances.

[1] The City of Winnipeg, by-law No. 7610/2000, *Winnipeg Police Service Regulation By-Law* (2000)

## Number of Responsive Records

The WPS indicated that there were 177 responsive records located and that the records are between 1 and 210 pages each. The WPS indicated that it originally considered issuing an Estimate of Costs, which was eventually decided against because it was determined to be unfair to the applicant as they would only receive non-substantive information.

Our office notes that considerations such as this are an example of a public body meeting part of its duty to assist under FIPPA. We agree that it would not be appropriate for a public body to have an applicant pay a fee estimate knowing the applicant would not receive substantive information at the end of the process.

We believe that it would also have been appropriate for the WPS, having reached this assessment, to speak with the applicant to discuss what information they might receive and whether they still wished to pursue the access requests.

Earlier in our discussions with the complainant, our office asked them if they would be willing to pay a fee in relation to their access request or if the need to pay a fee would affect their decision to proceed with this matter. The complainant indicated that they would be willing to pay a fee if required and were still interested in proceeding, provided they could receive some information. We shared this information with the WPS.

However, given the time since the access requests were made and the opportunities the public body would have had throughout the process to issue a revised access decision and a fee estimate, if necessary, our office's position is that it would no longer be fair to the complainant for the WPS to require fees to process the requests.

## Unreasonable Demand on WPS Operations

The WPS stated that, due to the nature of the records and the number of them, it would be an unreasonable demand on its operations to determine which files are open or may be re-opened. As mentioned above, natural justice and procedural fairness require the WPS to have a set time limit for when it is reasonable to consider an investigation open or subject to appeal or further consideration.

The WPS has indicated that it marks complaints as complete or closed, which should make it apparent which investigations are open, and which are not.

Additionally, while the WPS would be unable to accurately predict whether a file would need to be re-opened in the future, there is a point where it would no longer be reasonable for the WPS to do so.

The PSU should have policies and procedures setting out the process for its investigation of complaints, including when re-opening a closed investigation is no longer feasible or reasonable.

The WPS did not link this part of its representations to a provision of FIPPA. However, section 13 of FIPPA is the only section which uses wording similar to the wording used by the WPS here. Clause 13(1)(d) authorizes public bodies to disregard an access request if responding to that access request would unreasonably interfere with the public body's operations.

When these requests were made in 2021, there was a similar provision, clause 13(1)(b), that authorized public bodies to disregard, but it applied only to situations where two criteria were met: 1) the requests needed to be repetitious or systematic; and 2) they also needed to unreasonably interfere with the public body's operations.

The section was amended, and the new wording came into force in 2022. The new wording does not apply in this case as these requests must be considered based on the wording of the sections as they were written when the requests were made.

While section 13 of FIPPA authorizes public bodies to disregard requests for access in certain circumstances, it is not clear how these requests meet the requirements for this section. Furthermore, disregarding a request is a discretionary decision, which requires careful consideration of all relevant factors beyond simply establishing that the condition for disregarding is fulfilled.

# ANALYSIS

Exceptions to access in FIPPA fall under two categories, mandatory exceptions and discretionary exceptions. Mandatory exceptions to access are found in Division 3 of FIPPA and are those where public bodies are required to withhold information. Discretionary exceptions are found in Division 4 of FIPPA and give public bodies the choice of releasing information.

The general test for determining whether a section applies to the information in a record has two parts.

First, the public body must determine if the information is of the type described in the exception. Second, the public body must look at whether there is a limit to the exception that means that the information must still be disclosed in certain circumstances.

Mandatory exceptions set out specific types of information or circumstances where disclosure would be unreasonable/harmful and also includes limits to those types of information or circumstances.

For example, disclosing information that was provided in confidence by another government is generally prohibited, except if the record is more than 20 years old or the other government consents to its release.

In addition to the two steps set out for mandatory exceptions, there is another step for discretionary exceptions. When applying a discretionary exception, the third step is that the public body must consider whether it is appropriate to disclose the information, even though an exception may apply.

This is the act of exercising discretion. Many discretionary exceptions are explicitly harms-based; and all discretionary exceptions require the public body to consider all relevant factors when deciding whether or not to disclose the information, which would include consideration around whether the disclosure of that information could reasonably be expected to cause harm.

## The Application of Section 17 of FIPPA

At the outset, it is important to note that the complainant indicated in their access request that they were not requesting the identifiable personal information of members of the public or police officers.

In both the request for complaints and the request for compliments, the complainant stated, "*If possible, we'd like to see the [complaints/compliments] written in full spare information that may identify the complainant or the officer with the WPS.*"

Given the position of the complainant, our first step was to determine whether information in the records is personal information as defined by FIPPA.

Section 1 of FIPPA defines several terms used throughout the act, including "personal information". Specifically, it starts with the requirement that for information to be "personal information" it must be recorded and about an identifiable individual.

> *"**personal information**" means recorded information about an identifiable individual, including…*

The definition then lists several types of information, such as an individual's name, health information or work history that would clearly be personal information, provided the information is about an identifiable individual, or can be used to identify an individual. While this list is not exhaustive, it does give context for the types of information considered to be "personal information".

There is no question that the unsevered records contain personal information of identifiable individuals. The next step is to consider whether that information is subject to exceptions in section 17 and if so, whether the records can reasonably be severed such that they do not identify individuals.

Section 17 of FIPPA provides a mandatory exception to access that is specific to personal information. Subsection 17(1) sets out the basic principle that personal information should not be disclosed if it is an unreasonable invasion of a third-party individual's privacy.

> ***Disclosure harmful to a third party's privacy***
> ***17(1)*** *The head of a public body shall refuse to disclose personal information to an applicant if the disclosure would be an unreasonable invasion of a third party's privacy.*

Subsection 17(2) provides a list of the types of personal information, the disclosure of which is deemed to be an unreasonable invasion of privacy.

The WPS specifically cited clauses 17(2)(b) and 17(2)(e) in their representations.

> ***Disclosures deemed to be an unreasonable invasion of privacy***
> ***17(2)*** *A disclosure of personal information about a third party is deemed to be an unreasonable invasion of the third party's privacy if*
>
> *(b) the personal information was compiled and is identifiable as part of an investigation into a possible violation of a law, except to the extent that disclosure is necessary to prosecute the violation or to continue the investigation;*
>
> *(e) the personal information relates to the third party's employment, occupational or educational history;*

For information that is not described in subsection 17(2), subsection 17(3) sets out a non-exhaustive list of factors that must be considered when trying to determine whether the disclosure of information would unreasonably invade an individual's privacy.

And finally, subsection 17(4) sets out types of information and circumstances where the disclosure of personal information is not unreasonable, even where it would otherwise be required to be withheld under subsection 17(2).

In its representations, the WPS correctly stated that members of the public have an expectation of privacy when it comes to complaints and compliments submitted to the WPS. As noted above, the complainant has stated from the outset that they are not requesting any information that could identify a member of the public or an employee of the WPS.

An individual is identifiable if the information in the record, when combined with information otherwise available, could reasonably be expected to allow the individual to be identified.

If the process of removing the information means the individual is no longer reasonably expected to be identified, then the record can be severed, and the remaining information can be released.

Our office reviewed a recent decision made by the Manitoba Court as part of our investigation into this matter, *Annable (CBC) v. City of Winnipeg*[2] (*Annable*). In this case, the Court considered the City of Winnipeg's (the City) decision to disclose information regarding WPS members' service defaults but sever individual disciplinary penalties that correspond with the defaults on the basis that releasing the information would be an unreasonable invasion of the WPS members' privacy.

The City argued that even with the police officers' names removed, there were enough details in the penalties to allow others, specifically other employees of the WPS and the family members of the police officers, to identify the police officers involved.

The Court found that the disclosure of penalties in conjunction with other information that may be known about the police officers involved was not enough information to identify individual officers and ordered the City to release the previously severed disciplinary penalty information to the Appellant.

In Annable, Justice Martin clarified the test for disclosure under section 17. Specifically, Justice Martin stated that the test has two key components:

1. Is the information personal information about an identifiable individual?

2. Would the disclosure of the information be an unreasonable invasion of the individual's privacy?

At paragraphs 31 to 33 of Annable, Justice Martin outlined two considerations for determining whether information is personal information about an identifiable individual:

1. whether the information is about, or speaks to, an identifiable individual; and

2. whether the information can reveal or identify the individual.

With respect to the first consideration, if the information is uniquely related to a certain individual, then it is about an identifiable individual. Some of the records we reviewed as part of our investigation clearly identified an involved individual, either by use of their name or badge number. Other records included information that, when combined with other details, could potentially be used to identify an individual.

[2] *Annable (CBC) v. City of Winnipeg*, 2022 MBKB 222 (CanLII), <https://canlii.ca/t/jt67s>, retrieved on 2023-10-31 [*Annable*]

With respect to the second consideration, the Court confirmed that the test for determining whether information can reveal or identify an individual is whether there is a reasonable expectation that the individual can be identified.

Justice Martin clarified the second step of the test using the analytical framework described by Barbara von Tigerstrom in *Information and Privacy Law in Canada*[3]:

> *In order for information to qualify as personal information, it must be possible to identify the individual subject or subjects of the information. … The test that has long been used in Ontario is whether there is a "reasonable expectation that the individual can be identified" from the information that is disclosed. This must be demonstrated on a balance of probabilities, and the evidence may vary from case to case.*

Justice Martin further considered what a reasonable expectation would be at paragraph 36:

> *All in, a reasonable expectation standard means something considerably higher than a mere possibility, but lower than a probability, of an outcome occurring (such as identifying an individual). The evidence must be based on reason, on real and substantial grounds when looked at objectively, not matters that are fanciful, imaginary, contrived, or speculative.*[4]

The Court further states at paragraph 33 that a reasonable expectation analysis must consider all of the information that is disclosed or publicly available.

Our office noted the requirements set out in the *Annable* case to the WPS during our discussions on this case. The WPS responded in its representations and stated that an "analysis required to protect personal information requires a prospective component for the purpose of prevention of unreasonable invasion of individual privacy." The WPS cited *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*[5] (*Public Safety*) as the basis for this position.

---

[3] Barbara von Tigerstrom, *Information and Privacy Law in Canada*, (Toronto: Irwin Law Inc., 2020) at 210.
[4] *Annable*, *supra* note 3, at para 36.
[5] *Canada (Information Commissioner) v. Canada (Public Safety and Emergency Preparedness)*, 2019 FC 1279 (CanLII), <https://canlii.ca/t/j35r2>, retrieved on 2023-11-01

Specifically, the WPS cited paragraph 53 of *Public Safety*, which states:

> *I agree that standards and approaches applicable to section 20 of the ATIA are not necessarily applicable to section 19, given the different nature of the interests at stake in the two sections. At the same time, however, the "serious possibility" of Gordon and the "reasonable to expect" of NavCanada both appear to convey effectively the same standard: a possibility that is greater than speculation or a "mere possibility," but does not need to reach the level of "more likely than not" (i.e., need not be "probable" on a balance of probabilities). Applying such a standard recognizes the importance of access to information by not exempting information from disclosure on the basis of mere speculative possibilities, while respecting the importance of privacy rights and the inherently prospective nature of the analysis by not requiring an unduly high degree of proof that personal information will be released.*

Our office agrees that privacy and access rights must be considered harmoniously. Access is the general rule, but the personal information exception must not receive a "cramped interpretation". [6]

The balancing of these rights is reflected in s.17 which contains a large number of considerations to determine whether the release of personal information would be an unreasonable invasion of privacy. Both access provisions and privacy provisions must be given a full interpretation.

Our office also reviewed the Federal Court of Canada case, *Cain v. Canada (Health)*[7] (*Cain*). *Cain* relates to a refusal by Health Canada to release all but the first letter of postal codes and refusing to release the names of any cities from licensing records for growing medical marijuana. Much of the discussion in *Cain* centered around whether the second and third letters of postal codes could reasonably be expected to identify individuals.

The concern related to the fact that each character in a postal code further specifies the location it is attached to.

[6] *Dagg v. Canada (Minister of Finance)*, 1997 CanLII 358 (SCC), [1997] 2 SCR 403, <https://canlii.ca/t/1fr0r>, retrieved on 2023-10-31
[7] *Cain v. Canada (Health)*, 2023 FC 55 (CanLII), <https://canlii.ca/t/jv8b7> retrieved on 2023-12-04

For example, the postal code for our former Winnipeg office is R3C 3X1. The R indicates the office is in Manitoba, the 3 indicates it is in an urban area and the C specifies that area as downtown Winnipeg. The last three characters specify even further by indicating anything from a specific block to a specific building depending on the number of addresses in that location.

The Court was considering whether the release of this information, along with other information that was publicly available, would allow the applicant to identify the individuals mentioned in the records. The Court quotes Justice Gibson in *Gordon v Canada (Health)*[8] which states, at paragraph 34:

> "*Information will be about an identifiable individual where there is a* **serious possibility** *that an individual could be identified through the use of that information,* **alone or in combination with other available information."**
>
> (emphasis added by the Court in *Cain*)

Justice Pentney in *Cain* states that the onus is on Health Canada to establish that it was authorized to refuse to disclose the information in the records. The Court recognized that the right of access to information must be balanced against the right to privacy.

The Court reviewed an expert report which considered the risk that individuals could be identified under two assumptions, a "permissive" assumption where the applicant does not know the individuals in the dataset and a "conservative" assumption where the applicant either knows who is in the dataset or a specific individual in the dataset.

These assumption models can help set up a range of potential risk of identification, depending on the knowledge available to the public. The *Cain* expert did not provide an opinion on which of these assumptions should be applied because "*there are reasons for each of these assumptions to be reasonable ones…*"[9] Justice Pentney set out several factors he considered when determining which assumption should be applied.

The first is how sensitive the information is. In the *Cain* case, the information that could be linked to an identifiable individual was that they used medical marijuana. This information relates to an individual's health and the health care they are receiving, which is among the most sensitive type of information there is.

---

[8] *Gordon v. Canada (Health)*, 2008 FC 258 (CanLII), <https://canlii.ca/t/1vxt3>, retrieved on 2023-12-04
[9] *Cain, supra*, note 9, at para. 143.

The second factor the Court considered is the confidentiality of the types of information that could be used to link previously available information with information in the records. Information such as an individual's home address, gender or age range could be known or assumed by everyone who knows the individual or lives near them. The less confidential the disclosed information, the broader the range of people who could link it to other available information.

The final factor the Court considered is the potential motivation for the request for access. In the *Cain* case, there was a pattern of requests by the involved applicants as well as an interactive map which had been created and placed online, which suggested a certain level of motivation.

The Court also summarized several key concepts which the expert's methodology relied on. This includes the concept of "learning something new", which the Court set out in paragraph 78 of *Cain*:

> *the risk of disclosure only pertains to information that would add to the adversary's[10] existing knowledge; if the relevant information is already known to the adversary, even though it may technically be categorized as personal information, the risk of releasing that particular data is not meaningful*

The Court also mentioned the "mosaic effect". This concept has been discussed at length in the Canadian courts. It is used to describe how information which, in isolation, appears meaningless or trivial, could be compared to develop a more comprehensive picture.

As mentioned in the *Public Safety* case cited by the WPS, the "reasonable expectation" test used in *Annable,* and the "serious possibility" test used in *Cain* are effectively the same. Public bodies must be able to show that there is more than a mere possibility that an individual could be identified, but do not need to reach the level of a balance of probabilities.

Concepts like the mosaic effect or assumptions like those mentioned by Justice Pentney set out the analysis required under FIPPA and explain why our office requires public bodies to do line-by-line reviews of the responsive records.

---

[10] The term "adversary" in *Cain* has a specific definition which is explained by Justice Pentney at paragraph 73: "the expert uses the term "adversary" in a somewhat unusual way; it does not refer to an opponent or enemy (as the term is generally understood), but rather simply refers to someone who may seek to use the data that is released, whatever their motivation."

Each situation is specific and determining whether discrete items of information are about an identifiable individual and therefore required to be redacted would depend on the circumstances of each situation.

Turning to the information at issue in the current case, the WPS stated in its access decision "a sample of a complaint and a compliment were reviewed." Our office understands that to mean that the WPS initially reviewed a sample of one complaint and one compliment to determine whether severing was possible.

As was mentioned previously, our office reviewed two sample groups of records provided by the WPS, which in aggregate constituted 18 of the 177 responsive records originally identified by the WPS. When we reviewed the first sample (nine records), we agreed that much of the information in these records would have to be severed so that the persons who made the complaints/compliments could not be identified.

Most if not all of the scenarios described in these records were highly distinctive and possibly unique in some cases. These are factors which tend to make it easier to identify individuals, even in the absence of more obvious identifiers such as names, contact information and locations etc. Due to the nature of the severing likely required for these records, only disconnected bits of information would be left, which is not considered reasonable severing under FIPPA.

The second sample (also containing nine records) we reviewed was different. The complaints and compliment in this sample also included some personal information that would need to be severed. However, our office determined that reasonable severing was possible for many of the records from the second sample.

Based on our review of the records, we concluded that some of the information, if disclosed, could reasonably be expected to identify the individuals involved. However, in some cases, we found that once the obviously identifying information was removed, the remaining information could not reasonably be expected to identify the individuals involved.

Whether something will identify an individual or not depends not only on the record itself, but also on the number of details otherwise available to the person who receives the information.

The WPS noted in its representations that in other cases, information disclosed by its office has enabled applicants to identify the police officers involved even after clearly identifying information was severed from the records. The WPS also provided specific details of one of these incidents for our review.

In that case, the applicant was able to determine the name of one of the involved parties included in the responsive records and link that to other information from the responsive records. However, our office notes that the information that permitted the individual to be identified was publicly available prior to the access decision being made. While the applicant was able to identify the individual, this did not lead to the applicant gaining new information about the individual.

When determining whether an individual is identifiable, public bodies must consider the full context of the information available both in the responsive records and from other public sources. In relation to the case given as an example by the WPS, our office agrees that there likely was a reasonable expectation that, even with the limited details provided, the individual could be identified.

However, public bodies must then consider the second part of the test under section 17, as clarified by *Annable,* and determine whether the disclosure of that information unreasonably invades the privacy of the individual.

This is done by first considering whether subsection 17(2) applies to the information. If 17(2) applies, then the public body must consider subsection 17(4). If 17(2) does not apply, then it must consider whether the factors listed under subsection 17(3) would make the disclosure of the information an unreasonable invasion of privacy.

In the example case, there were public records which contained the information in the responsive records and there are clauses of both 17(3) and 17(4) of FIPPA which could potentially permit disclosure of that information.

Whether or not the disclosure of information that is publicly available is an unreasonable invasion of an individual's privacy depends on the specific circumstances and must be determined on a case-by-case basis.

Our office does not accept that the existence of situations where individuals have been identified through the release of records by the public body means that the release of any information related in any way to an individual (after severing has been applied) meets the reasonable expectation standard set out in *Annable*.

The WPS has not shown that there is a reasonable expectation that the release of some information, after the names, contact information and some other specific information, such as location, have been removed, would identify the individuals involved in all of the responsive records.

Additionally, if the WPS takes the position that the release of specific types of information could reasonably be expected to lead to the identification of an individual, then it would need to give reasons to explain why it believes that type of information could be used to identify the individual.

How specific the reasons would need to be or what type of evidence would be required would depend on the nature of the information the WPS was seeking to redact. Deciding to redact information that could apply to a wide range of individuals may need more specific reasons than information that applies only to specific and limited numbers of people.

The balancing of privacy rights with access rights requires public bodies to consider the risks to these rights caused by both the disclosure and the refusal of access to information.

This is done by conducting a line-by-line review of the responsive records and considering what other information is available to the public. Items of information must be considered in their own right, and a specific type of information might be redacted in one record and disclosed in another.

The representations provided by the WPS do not show that it made these considerations. The WPS has not identified specific pieces or types of information it believes would identify the individuals named in the records. It has not given examples of how more general information found in the records could be used to identify the individuals.

Given the above considerations, our office finds that the WPS was not authorized to refuse access in full under section 17 of FIPPA.

## Reasonable Severing of the Records

As discussed above, the purpose of FIPPA is to allow individuals access to information in the custody or control of public bodies. While access to information is the starting point, FIPPA recognizes that some information should be kept confidential, including for the reason of protecting the privacy rights of third parties.

FIPPA balances these competing rights through limited exceptions to access and a requirement to sever information from a record to allow for as much information as reasonably possible to be provided to an applicant. Subsection 7(2) sets out this requirement:

> **Severing information**
> **7(2)** *The right of access to a record does not extend to information that is excepted from disclosure under Division 3 or 4 of this Part, but if that information can reasonably be severed from the record, an applicant has a right of access to the remainder of the record.*

Subsection 7(2) of FIPPA requires that where an exception applies to a portion of the information in a record, only that portion is severed.

The applicant is entitled to access to the remainder of the record unless an exception in another section of FIPPA applies. This severing is required to be reasonable and ensure that only the minimum amount of information necessary is severed while also ensuring that the information provided is meaningful and not disconnected pieces of information.

Our office reviewed samples of the records to determine whether they could be severed to allow for the partial release of the records. In our analysis of whether the WPS conducted reasonable severing, we heeded Justice Martin's caution in Annable that there are over 1300 individual officers to whom the information could relate, and that the "mosaic effect" should be employed sparingly.

As explained earlier, the mosaic effect is a concept that explains how information that seems to be non-identifiable on its own can be combined with other information to identify an individual.

However, we also acknowledge that, unlike in Annable, in this case, the complaints and compliments sometimes provide unique details that could be combined with other information to reasonably lead to the identification of involved individuals, if disclosed.

Based on our review, while there are some records where reasonable severing would not be possible, there are others where the personal information of identifiable individuals could reasonably be severed from the records to allow the complainant access to at least some of the information. Given the above considerations, our office finds that the WPS did not meet the requirements of subsection 7(2) of FIPPA.

## The Potential Application of s. 24 and 25 to the Responsive Records

In the public body's representations, the evidence and discussion related to sections 24 and 25 was the same. As such, our office will review these sections together. Sections 24 and 25 of FIPPA are discretionary exceptions to access which authorize a public body to refuse access to information that could harm individual or public safety, law enforcement or legal proceedings.

The WPS specifically cited subsection 24(a) and clauses 25(1)(a) and 25(1)(e) in its representations.

> **Disclosure harmful to individual or public safety**
> **24** *The head of a public body may refuse to disclose to an applicant information, including personal information about the applicant, if disclosure could reasonably be expected to*
>
> *(a) threaten or harm the mental or physical health or the safety of another person;*
>
> **Disclosure harmful to law enforcement or legal proceedings**
> **25(1)** *The head of a public body may refuse to disclose information to an applicant if disclosure could reasonably be expected to*
>
> *(a) harm a law enforcement matter;*
>
> *(e) endanger the life or safety of a law enforcement officer or any other person;*

The purpose of these sections is to allow public bodies to refuse access to information in records if the release of the information could cause the specified harm(s).

When determining whether to refuse access under these sections, a public body must also consider whether doing so is an appropriate exercise of its discretion in the circumstances.

In *Annable* the Court referenced the case of *Merck Frosst Canada Ltd. v. Canada (Health)*[11] (*Merck*). In *Merck*, the Supreme Court of Canada (SCC) clarifies the harms test required when applying a discretionary exception to access. The Court states that the test is a "reasonable expectation of probable harm."

In Merck, the SCC notes the importance of correctly interpreting this test as it can be applied to many exceptions to access in both the federal and provincial legislation. The Court states:

> *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.*[12]

Our office notes that the SCC specifically cited section 17 of the *Access to Information Act*[13] which does not have the exact same wording as section 24 of FIPPA but has a similar purpose.

> **Safety of individuals**
> **17** *The head of a government institution may refuse to disclose any record requested under this Part that contains information the disclosure of which could reasonably be expected to threaten the safety of individuals.*
>
> (emphasis added)

[12] *Merck*, *supra* note 5, at para 195.
[13] *Access to Information Act*, RSC 1985, c A-1, <https://canlii.ca/t/563rq> retrieved on 2023-11-02

The SCC set out the test as follows:

> *... A balance must be struck between the important goals of disclosure and avoiding harm to third parties resulting from disclosure. The important objective of access to information would be thwarted by a mere possibility of harm standard. Exemption from disclosure should not be granted on the basis of fear of harm that is fanciful, imaginary or contrived. Such fears of harm are not reasonable because they are not based on reason: see Air Atonabee, at p. 277, quoting Re Actors' Equity Assn. of Australia and Australian Broadcasting Tribunal (No 2) (1985), 7 A.L.D. 584 (Admin. App. Trib.), at para. 25. The words "could reasonably be expected" "refer to an expectation for which real and substantial grounds exist when looked at objectively": Watt v. Forests, [2007] NSWADT 197 (AustLII), at para. 120. On the other hand, what is at issue is risk of future harm that depends on how future uncertain events unfold. Thus, requiring a third party (or, in other provisions, the government) to prove that harm is more likely than not to occur would impose in many cases an impossible standard of proof.*[14]
>
> (emphasis added)

Given the test as set out in Merck and the requirements of FIPPA, in order for a discretionary exception to access to apply to information in a responsive record, the following factors must be present:

1. The information must be of the type referenced in the exception.

2. There must be a reasonable expectation of probable harm.

3. The harm must be caused by the disclosure of the information.

The WPS routinely severs the names of police officers under section 25 and our office has found in the past that, in most circumstances, the WPS is authorized to do so. There are limited exceptions to this, such as the names of police officers who hold executive or public facing positions, such as the Chief of Police or the public information officer, whose names and faces regularly appear in the media.

[14] *Merck*, *supra* note 5, at para 204.

In relation to the application of sections 24 and 25, the WPS stated that the release of the records, specifically the complaints, could harm the mental and physical health of police officers. The WPS set out numerous factors in support of its position, including the outcomes of research on officer stress. The WPS also provide specific information related to the general stress and mental health of police officers in the WPS.

Lastly, the WPS also stated that some of the complaints were determined to be unsubstantiated and compliments are not tracked in the same manner as complaints, which means that it appears that there are significantly more complaints than compliments.

The WPS stated that these factors would increase the negative perception of the responsive records and amplify the harm to police officers' physical and mental health.

Public bodies routinely include information that clarifies or explains responsive records, and the potential inaccuracies within them when issuing access decisions. In fact, subsection 14(2) of FIPPA expressly permits a public body to give an applicant any additional information that the public body believes may be necessary to explain a record.

The potential for someone to misunderstand information in the records is not sufficient evidence to show that harm will be caused by the release of the same.

Our office accepts that there are a number of factors that can have a negative effect on the mental and physical health of police officers. However, the WPS has not provided any evidence that the release of the specific information in the responsive records could be reasonably expected to harm the mental and physical health of its members.

Returning to the test as it was set out in *Merck*, is there a reasonable expectation that the release of de-identified copies of the responsive records would cause probable harm? The WPS has provided research to support that the negative perception of police in the media can cause harm to police officers.

However, there has been no evidence presented to show that the release of any specific information within the records created an expectation of harm "for which real and substantial grounds exist". Rather the WPS made a statement about the possible impacts of the release of the records as a whole on members of the WPS generally.

The proper application of FIPPA requires a line-by-line review of the responsive records. Each specific piece of information in the record must be examined to determine what, if any, exceptions to access might apply. If a public body refuses access to an entire record, it must still be able to explain its reasons for severing each specific section of the record, be it a sentence or paragraph.

For sections 24 and/or 25 to be applied to the information in the responsive records, the WPS would have to show not only that there exists a reasonable expectation of probable harm but that the harm would be caused by the disclosure of the information.

In this specific case, the WPS would have to provide evidence that the disclosure of the information in the responsive records could reasonably be expected to exacerbate or otherwise increase the current risk to the mental and physical health or safety of police officers or to a matter of law enforcement.

If the release of information would have no substantive effect on the harm as it currently exists, then there is no reasonable expectation that the disclosure itself would cause probable harm.

## The Potential Application of s. 29.2 to the Responsive Records

Lastly, the WPS indicated in its representations that it considers information in the responsive records to be subject to section 29.2 of FIPPA. However, section 29.2 of FIPPA came into force after the access requests were made.

These access requests and the associated complaint must be reviewed and addressed under the version of FIPPA that was in force at the time the requests were made. The WPS has no jurisdiction to refuse access to the records under section 29.2.

Our office is briefly discussing the application of section 29.2 in this report to share our general understanding of the section and how and when it will apply to information.

The wording of section 29.2 applies to information that relates to an ongoing investigation or information that was created or collected for the purpose of an investigation.

***Information relating to workplace investigations***

***29.2*** *The head of a public body may refuse to disclose information to an applicant if*

*(a) the information relates to an ongoing investigation by or on behalf of the public body into the employment-related conduct of an employee; or*

*(b) the information was created or collected for the purpose of such an investigation, regardless of whether the investigation took place, and disclosure of the information could reasonably be expected to cause harm to the applicant, a public body or a third party.*

For section 29.2 to be applied to information in responsive records similar to those requested here, a public body would have to provide evidence that the records were created with the understanding that an investigation would occur. Comparable to the requirements for records protected under litigation privilege, public bodies need to show that the records were created or collected either because there was an investigation ongoing or there was a reasonable expectation that one would be conducted.

Additionally, the investigation would need to be one conducted by or on behalf of the public body. For example, complaints that the WPS forwards to another organization, such as the Independent Investigations Unit or the Law Enforcement Review Agency, would not be workplace investigations, conducted by or on behalf of the public body, as described in the section.

Finally, as discussed in other sections of this report, the public body would need to consider whether there is a reasonable expectation of probable harm and whether refusing to disclose the information was an appropriate use of its discretion before any redactions could be made under section 29.2.

# FINDINGS

Based on the above review of the evidence, representations of the complainant and the WPS, FIPPA and the case law, our office finds that the City of Winnipeg – Winnipeg Police Service did not fulfill the requirements of subsection 7(2) of FIPPA to reasonably sever the records responsive to the complainant's request. As such, the complaint is supported, and our office will be issuing recommendations to the public body.

# RECOMMENDATIONS

Based on our office's finding that the City of Winnipeg – Winnipeg Police Service did not meet the requirements of subsection 7(2) of FIPPA, the following recommendations are made:

**Recommendation 1:** The Ombudsman recommends that the City of Winnipeg - Winnipeg Police Service reconsider its decision to withhold the records in full and release the records, with the exception of information that could reasonably be expected to identify a WPS member or member of the public as outlined earlier in this report.

**Recommendation 2:** The Ombudsman recommends that the City of Winnipeg—Winnipeg Police Service conduct a line-by-line review of the records. In doing so, we recommend they apply reasonable severing to the information that could reasonably be expected to identify individuals, as discussed in this report.

**Recommendation 3:** Following the public body's reconsideration as described above, the Ombudsman recommends that the City of Winnipeg—Winnipeg Police Service issue a revised access decision to the complainant under section 12 of FIPPA and release the records with appropriate severing.

# HEAD'S RESPONSE TO THE RECOMMENDATIONS

Under subsection 66(4), the City of Winnipeg – Winnipeg Police Service must respond to the Ombudsman's report in writing within 15 days of receiving this report. As this report is being sent by email to the head on February 27, 2025, the head shall respond by March 14, 2025. The head's response must contain the following information:

> **Head's Response to the Report**
> ***66(4)*** *If the report contains recommendations, the head of the public body shall, within 15 days after receiving the report, send the Ombudsman a written response indicating*
>
> *(a) that the head accepts the recommendations and describing any action the head has taken or proposes to take to implement them; or*
>
> *(b) the reasons why the head refuses to take action to implement the recommendations.*

## Ombudsman to Notify the Complainant of the Head's Response

When the Ombudsman has received City of Winnipeg – Winnipeg Police Service's response to her recommendations, she will notify the complainant about the head's response as required under subsection 66(5).

## Head's Compliance with Recommendations

If the head accepts the recommendations, subsection 66(6) requires the head to comply with the recommendation within 15 days of acceptance of the recommendations or within an additional period if the Ombudsman considers it to be reasonable.

Accordingly, the head should provide written notice to the Ombudsman and information to demonstrate that the public body has complied with the recommendations and did so within the specified time period.

Alternatively, if the head believes that an additional period of time is required to comply with the recommendations, the head's response to the Ombudsman under subsection 66(4) must include a request that the Ombudsman consider an additional period of time for compliance with the recommendations. A request for additional time must include the number of days being requested and the reasons why the additional time is needed.

February 27, 2025
**MANITOBA OMBUDSMAN**[15]
300 - 5 Donald Street, Winnipeg, MB R3L 2T4
1-800-665-0531 | ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca
Available in alternate formats upon request.

[15] The Manitoba Ombudsman has delegated the authority to issue this report to Manitoba's Deputy Ombudsman under section 56 of The Freedom of Information and Protection of Privacy Act due to a declared perceived conflict of interest.