Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Access to Information and Privacy Implementation Notice 2024-01: Upholding privacy and safety of public servants

Published: 2024-11-11

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-84/2024E-PDF
ISBN: 978-0-660-74620-3

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Avis de mise en œuvre de l’accès à l’information et de la protection des renseignements personnels 2024 01 : Protéger la vie privée et la sécurité des fonctionnaires

Access to Information and Privacy Implementation Notice 2024-01: Upholding privacy and safety of public servants

1. Effective date

This implementation notice takes effect on November 13, 2024.

2. Authorities

This implementation notice is issued pursuant to paragraph 70(1)(c) of the *Access to Information Act* (ATIA) and paragraph 71(1)(d) of the *Privacy Act*.

3. Purpose

This implementation notice is meant to guide institutions' Access to Information and Privacy (ATIP) offices in managing and processing delicate access to information (ATI) and personal information requests where the information sought causes a public servant to fear for their safety because of who they are, and not the type of work they do. The requests seek information that may infringe on the personal lives of officers or employees of the government institution. This notice also provides guidance regarding

situations where there is concern that if the requested information were acknowledged or disclosed, it could be used to threaten the life, bodily integrity and psychological health and safety of a public servant.

4. Context

4.1 Concerns raised by employees

Employees of the public service who are members of equity-seeking groups (in other words, those facing discrimination as defined in the *Canadian Human Rights Act*), have raised concerns that individuals may be submitting ATIP requests with the specific aim of harassing them. These requests have caused these employees to express fear for their safety and well-being.

Other ATIP requests have been submitted under the guise of seeking government records, but the perceived intention of the requester was to intimidate an employee with whom they have an unhealthy personal relationship.

Finally, in some cases, unbeknownst to the requester, the responsive records contain information that could raise safety concerns for employees if they were disclosed. For example, an employee who has a restraining order against someone may not want their work locations disclosed.

4.2 Purpose of the *Access to Information Act*

The purpose of the ATIA is set out in section 2 of the Act:

> ...to enhance the accountability and transparency of federal institutions in order to promote an open and democratic society and to enable public debate on the conduct of those institutions.

To further this purpose, subsection 2(2) of the ATIA permits requests under Part 1 of the Act. It is a quasi-constitutional statute that promotes accountability and transparency. However, in certain circumstances the right of access is ceded to other interests, one of them being the protection of privacy. The Department of Justice notes that "the protection of the privacy of personal information constitutes one of the most important exceptions to the right of access." [1]

To balance the protection of privacy with the transparency obligations in ATIP requests, there are exceptions to the definition of personal information for officers and employees of government institutions. The exceptions reflect the fact that there is certain information which, barring other considerations, the public has a right to know. However, public servants do not forsake all their rights to privacy despite their choice of employer, as was contemplated in *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 at paragraph 8.

In practice, records often contain both personal information and personal information that falls within the exceptions set out in the *Privacy Act*. Institutions may want to more forcefully uphold the decision in *Terry v. Canada (Minister of National Defence)*, [1994] T-845-94, [2] where the Court relied on the rule of interpretation known as *expressio unius est exclusio alterius*, which means "the expression of one thing is the exclusion of the other." Under this rule, in order to fall within the exception set out in paragraph 3(j) of the *Privacy Act*, the information requested must fall squarely within it. When the substance of the record is skewed more heavily toward the individual, rather than toward the general characteristics associated with their position or functions, it becomes more likely that the information is personal and not captured in the exception, and less likely that severability is feasible, because the risk of re-identification is increased. [3]

In their exercise of discretion to not disclose, institutions can factor in whether the request has a purpose contrary to subsection 2(2) of the ATIA. This includes when requests are to ascertain information about public servants that relates to the prohibited grounds for discrimination or to harass them.

4.3 Employee needs

As an employer, the federal public service has a duty under section 124 and subsection 125(1) of the *Canada Labour Code* to ensure that the health and safety at work of every employee is protected through the prevention of accidents, occurrences of harassment and violence and physical or psychological injuries and illnesses. Public servants must be able to do their jobs, including responding to ATIP requests, without fear for their well-being and safety and without fear that their privacy will be infringed on. They also must be able to share with their employer, or with trusted individuals, their needs in the workplace. They should be able to express feelings and concerns, and have that information protected from disclosure. There may be scenarios in which an employee may share uniquely personal information with their employer in the course of their employment. Finally, there are provisions for the acceptable personal use of electronic networks and devices during personal times (for example, during breaks and lunch) provided that the uses do not interfere with official responsibilities or the conduct of regular business operations.

5. Guidance

5.1 Considerations

When processing ATIP requests that cause a public servant to fear for their safety because of who they are, not because of the work that they do, consider the following:

- the notion of control

- the provision on declining to act (section 6.1 of the ATIA)
- the existence of a record not required to be disclosed (subsection 10(2) of the ATIA, subsection 16(2) of the *Privacy Act*)
- the exemptions set out in sections 17 and 19 of the ATIA and in sections 25 and 26 of the *Privacy Act*
- internal consultations

5.1.1 Notion of control

In accordance with subsection 4(1) of the ATIA and paragraph 12(1)(b) of the *Privacy Act*, the right of access to information under these Acts only applies to records under the control of government institutions. An important first step in the test of control is whether the contents of the records relate to an institutional matter, in other words, whether they are relevant to the mandate, obligations, operations and functions of the institution. The Acts are not intended to capture records about non-institutional matters in the physical possession of federal institutions. For example, they are not intended to capture records relating to the case of an employee who is feeling unsafe at home and who therefore uses their work email account to seek assistance or legal advice. Another example would be the non-work-related uses of government issued devices that are permitted in accordance with Appendix A of the *Directive on Service and Digital*. Because of these permissible uses, information unrelated to work matters is found on work servers. This was the case in the *City of Ottawa v. Ontario*, 2010 ONSC 6835.

While the case law indicates that emails of a personal nature of government employees are generally not under the control of an institution, if any information contained in these emails was used for purposes relating to the institution's mandate (such as what could be broadly captured as human resources activities) the finding on control might be different. This could be the case, for instance, if the requested emails relate to an investigation

conducted into possible misuses of government electronic resources or to a conflict of interest, or if the emails relate to employment matters, such as a sense of safety in the workplace.

Institutions that receive ATI requests are required to conduct reasonable searches for responsive records under their control. If there is a question as to whether certain records are, in fact, under an institution's control, the institution's delegated officials under the ATIA and *Privacy Act* must review the records and make a determination on control. Responsibility for making this determination rests solely with the institution's delegated officials, who must be provided with the records; it does not rest with the institution's office of primary interest (OPI) or with anyone else.

Depending on the nature and sensitivity of the records, ATIP offices may have procedures in place to examine records but not retain any copies in their repository. These procedures would be similar to those in place for records in a minister's office. They ensure that the ATIP office does not have records that it does not have a right to possess or have custody over, should it be determined that the records are not under the control of the institution. Employees may keep private items at the place of work without them falling within the employer's possession and custody with respect to ATIP requests, and visual confirmation by the ATIP office can be sufficient. These items would be noted in the processing file. Further guidance on making determinations with respect to control can be found in the Access to Information Manual, the Personal Information Request Manual and the Information Commissioner of Canada's Interpretation Guide on the Control of Records.

5.1.2 Decline to act (section 6.1 of the *Access to Information Act*)

Section 6.1 of the ATIA provides that the head of a government institution may decline to act on an ATI request, with the Information Commissioner's written approval, if, in the opinion of the head of the institution, the request is:

- vexatious
- made in bad faith
- otherwise, an abuse of the right to make a request for access to records

Obtaining such approval could remove a requester's express right of access related to the request in question. Given the importance of the right of access, requests for approval to decline to act on an ATI request must be supported by clear and compelling reasons that are sufficiently detailed in the application.

In addition, institutions may only seek the Information Commissioner's approval to decline to act on an ATI request after having made every reasonable effort to help the requester with the request, as is required under subsection 4(2.1) (duty to assist).

The concepts of vexatiousness, bad faith and abuse are examined in turn in 2020 OIC 17, Order M-850 (Information and Privacy Commissioner of Ontario), and Order MO-4257:

> **Vexatiousness** is usually understood to mean intent to annoy, harass, embarrass, or cause discomfort. However, in the context of an application to decline to act on an access request, vexatiousness must rise above annoyance or inconvenience.
>
> **Bad faith** is usually understood to be the opposite of good faith. "Bad faith" generally implies a design to mislead or deceive another, not prompted by an honest mistake as to one's rights, but by some interested or sinister motive. "Bad faith" is not simply bad judgement or negligence, but rather implies the conscious doing of a wrong because of a dishonest purpose.
>
> **Abuse** is usually understood to mean a misuse or improper use.

Every application made to the Office of the Information Commissioner (OIC) to decline to act on an ATI request is considered on a case-by-case basis and is evaluated objectively. Evidence submitted to the OIC might include a documented history of repeated requests, communications between the ATIP Office and the requester (including whether these communications include abusive language), and public statements made by the requester regarding their ATI request.

For additional information, see the OIC's published guidance: Process: Seeking the Information Commissioner's approval to decline to act on an access request under section 6.1.

No provision equivalent to section 6.1 of the ATIA exists in the *Privacy Act*.

5.1.3 Existence of a record not required to be disclosed (subsection 10(2) of the *Access to Information Act*, subsection 16(2) of the *Privacy Act*)

Subsection 10(2) of the ATIA and subsection 16(2) of the *Privacy Act* provide that an institution may, but is not required to, indicate whether a record or personal information exists. In some situations, institutions may want to "neither confirm nor deny" the existence of a record or personal information by invoking subsections 10(2) or 16(2).

There may be scenarios where disclosure of the records or information requested could be injurious to the safety of an individual or infringe on their right to privacy but where there is no clear evidence that a request is vexatious, in bad faith or abusive. Rather, the request seems to seek records directly related to government information that should be available to the public, subject to limited and specific exemptions to the right of access. For example, the request may seek mentions of the requester during appointments with the Employee Assistance Program. Given the nature and content of the responsive records, it could, for example, put the safety and security of the employee at risk. This is a scenario where the request text is written in such a way that by acknowledging the existence or non-existence of a record, it could by itself disclose information to a requester.

When invoking these subsections, the institution must indicate the provision (exemption or exclusion) on which refusal of access to the record or personal information could reasonably be expected to be based, if it existed.

5.1.4 Exemption: personal information

Section 19 of the ATIA protects personal information, and section 26 of the *Privacy Act* protects the personal information about another individual.

Section 3 of the *Privacy Act* defines personal information as "information about an identifiable individual that is recorded in any form." Examples include information relating to an identifiable individual's income, DNA, sexual orientation, or political inclination. However, paragraph 3(j) of the *Privacy Act* includes an important exception to the definition of personal information when applying these two exemptions. Under paragraph 3(j), personal information does not include:

> **(j)** information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,
>
> > **(i)** the fact that the individual is or was an officer or employee of the government institution,
> > **(ii)** the title, business address and telephone number of the individual,
> > **(iii)** the classification, salary range and responsibilities of the position held by the individual,
> > **(iv)** the name of the individual on a document prepared by the individual in the course of employment, and
> > **(v)** the personal opinions or views of the individual given in the course of employment, ...

Government employees should therefore understand that what they communicate in the course of their employment may fall within the exception to the definition of personal information and could therefore be disclosed in an ATIP request. One example of an exception under paragraph 3(j) is a public servant's signature block, which (depending on what they choose to incorporate) often identifies how the public servant wants to be addressed in the workplace, including professional certifications, honorifics, and personal pronouns.

The name of an individual on a document and the personal opinions or views given in the course of employment generally fall within the exceptions set out in subparagraphs 3(j)(iv) and (v) of the definition of "personal information." However, there remains a reasonable expectation of privacy for employees or officers of a government institution for records that are uniquely personal in nature or performance related. [4] If the subject of an ATI request is directed in a manner to ascertain the gender identity of an individual or their individual job performance, or if the responsive records contain information of a private nature but peripherally still related to institutional matters, such as feelings about work, ATIP offices should consider applying subsection 19(1).

The exceptions to the definition of personal information are to be interpreted narrowly. The exceptions in paragraphs (j), (j.1), (k) and (l) reflect the fact that there is certain information about government employees, persons performing services under contract for a government institution, and discretionary benefits which, barring other considerations, the public has a right to know. They are not intended to serve as a glimpse into elements that are inherently personal that a public servant may have written in correspondence.

5.1.5 Exemption: safety of individuals

Section 17 of the ATIA and section 25 of the *Privacy Act* provide that the head of a government institution may refuse to disclose any records or information that contains information the disclosure of which could reasonably be expected to threaten the safety of individuals.

The types of individual safety interests that could be threatened are relatively broad, covering an individual's life, bodily integrity, and psychological health.

As set out in more detail in the Access to Information Manual and the Personal Information Request Manual, the type of information protected under this exemption may cover not only the name of the individual, but any identifier or other kind of information that is likely, by its release, either by itself or by a "mosaic effect," to threaten the safety of the individual.This could be information that either directly or indirectly reveals the identity, home address or other identifier of such an individual.

For an employee of a government institution, the exemption could cover information that is not normally protected information, such as the name of the individual's employer, place of employment, address of employment, or job title. The exemption may also apply to publicly available information that can be matched with other data to reveal information that could threaten the security of an individual.

When demonstrating the applicability of these exemptions, the institution must demonstrate that there is a reasonable basis for believing that disclosing the information will endanger an individual's safety.

The injury test might be satisfied with at least some evidence demonstrating that the likelihood is considerably more than mere speculation but somewhat less than "more likely than not" and that the safety of individuals is or will be threatened by the disclosure. This can be based on incidents where aggressive behaviour was directed at a specific person or people, the nature of an individual's employment, or details of actual threats.

5.1.6 Internal consultations

During the processing of a request, an OPI may provide records in response to a request that are administrative or routine in nature, such as access logs. The OPI may not be aware that employees who are implicated in the request have concerns related to their safety and may rely on previous advice given for similar requests or jurisprudence to recommend the disclosure of the records.

These scenarios are mostly likely to occur with requests containing personal information that falls within the exception of the definition for public servants. For example, in *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, the requester was seeking information on sign-in logs showing the number of hours spent in the workplace to inform the union with respect to collective bargaining. The court determined that the information fell within the exception of the definition of personal information and should be released to the requester. In that case, the requested information was intended to assist the position of employees with respect to their compensation. Some institutions may use *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403 to justify the disclosure of routine records such as sign-in logs, particularly where there is no indication that the information may be used to identify or target individual employees. However, regardless of how previous jurisprudence ruled on the interpretation and application of section 19 of the ATIA (or section 26 of the *Privacy Act*) or section 17 of the ATIA (or section 25 of the *Privacy Act*), the exemptions must still be considered on their individual merits with each new request.

ATIP offices may want to communicate with security officials in their organization to determine whether there are any imminent concerns within the institution, on a need-to-know basis. For example, security personnel may be aware of restraining orders related to an employee that may be relevant to an ATI request. If there are ongoing concerns for individual employees' safety, security personnel may want to compile a list of names of

individuals for limited distribution within the ATIP office. In the event the requested information includes an employee on the list, the ATIP office can consult with security personnel and recommend any relevant exemptions.

5.2 Communicating with employees and offices of primary interest

If at any point during the processing of a request under the ATIA or the *Privacy Act* an employee or an OPI identifies concerns about their safety and well-being, or about the safety and well-being of other individuals in relation to a request or the release of the responsive records, these concerns must be treated seriously and with compassion. The following guidance is intended to support ATIP analysts in addressing these concerns.

5.2.1 Be transparent and open during the processing of requests

To reassure employees that steps will be taken to ensure their safety and well-being, while still respecting the legal obligations under the Acts, ATIP analysts can:

- communicate the steps that will be taken to review the responsive records
- establish a clear understanding of the notion of control and how it relates to requests
- provide information on how exemptions are applied to records and which exemptions may be applicable (noting that the decision to disclose certain information remains at the discretion of the head of the institution or their delegate and will also depend on the context of the records being considered)
- work with the institution’s security and human resources to support the individual in alignment with the government’s responsibilities as the employer to prevent and protect against harassment and violence in the workplace
- follow up with the individual as to what was released

ATIP offices may leverage institutional supports to protect and reassure employees who feel endangered.

5.2.2 Discuss whether records or the request align with the purpose or scope of the Acts

Notion of control

In situations where employees have identified records in their possession that they do not believe relate to institutional matters but are captured in the scope of the request text, ATIP offices can help guide them through their internal procedures with respect to control. It is important to remind employees that these types of discussions may be documented in processing files to satisfy policy and directive requirements. This information may, in turn, be shared with either the Office of the Information Commissioner or the Office of the Privacy Commissioner in the event of a complaint under the respective Act.

Declining to act under the *Access to Information Act*

In situations where employees raise concerns with respect to their safety and well-being and the institution has evidence to support that an ATI request is vexatious, made in bad faith, or otherwise an abuse of the right to make a request for access to records, the head of the institution may consider seeking the Information Commissioner's written approval to decline to act on the request.

ATIP offices should ensure that the employees involved are aware of the steps to seek the Information Commissioner's approval to decline to act. First, institutions must make every reasonable effort to assist the requester in accordance with subsection 4(2.1) of the ATIA before seeking the Information Commissioner's approval to decline to act. When the government institution requests the Commissioner's approval, they must

give written notice to the requester of the suspended processing of the request. Finally, they must provide the results of the Information Commissioner's decision to the requester.

Existence not required to be disclosed

ATIP offices may want to explain to employees the possibility of neither confirming nor denying the existence of records in certain circumstances, depending on the wording of the request. A good example would be if the mere confirmation of records existing in response to a request would in itself reveal information that would otherwise qualify for exemption under a provision of the ATIA or the *Privacy Act*.

5.2.3 Access to information and privacy training and its interplay with information management best practices

Subsection 4.1.2 of both the *Directive on Access to Information Requests* and the *Directive on Personal Information Requests and Correction of Personal Information* requires that employees of government institutions, and officials who have functional or delegated responsibility for the administration of the Acts, receive training in accordance with Appendix B: Mandatory Procedures for Access to Information Training and Appendix B: Mandatory Procedures for Privacy Training. When delivering ATIP training, institutions can include a reminder to employees of the interplay between their right to privacy and the transparency obligations set out in the Acts, especially with respect to the exceptions to the definition of personal information set out in paragraph 3(j) of the *Privacy Act*. Good information management practices and adopting strong privacy protection principles are paramount for ensuring that employee information is properly siloed. When personal information is interwoven with records of business value, there is a greater possibility of its relevance as a responsive record in an ATIP request. This is especially common in emails, but the OIC has two suggested best practices on the subject:

- Keep personal (in other words, non-work related) messages separate: avoid having personal email messages captured as part of an ATI request by ensuring they are kept separate from email messages of business value
- Handle only one subject in every email string: resist the urge to request an update from your colleague on an unrelated project or file within an email string that is already started

However, if the records contain these types of scenarios, remind OPIs and employees that, where possible, the ATIP office will work with them to ensure their privacy is still protected.

6. Application

This implementation notice applies to government institutions as defined in sections 3 of the ATIA and the Privacy Act, including parent Crown corporations and any wholly owned subsidiaries. It does not apply to the Bank of Canada.

7. References

7.1 Legislation

- Access to Information Act
- *Canada Labour Code*
- *Privacy Act*

7.2 Related Treasury Board policy instruments

- Directive on Access to Information Requests
- Directive on Personal Information Requests and Correction of Personal Information
- Directive on Service and Digital
- Policy on Access to Information

- Policy on Privacy Protection

7.3 Related guidance instruments

- Access to Information Manual
- Personal Information Request Manual
- Investigation Guidance, Process: Seeking the Information Commissioner's approval to decline to act on an access request under section 6.1

8. Enquiries

Members of the public may contact TBS Public Enquiries for information about this implementation notice.

Employees of government institutions may contact their Access to Information and Privacy (ATIP) coordinator for information about this implementation notice.

ATIP coordinators may contact ippd-dpiprp@tbs-sct.gc.ca for information about this implementation notice.

Footnotes

1 *The Offices of the Information and Privacy Commissioners: The Merger and Related Issues*

2 Contact your legal services team to obtain a copy of this decision.

3 *Matas v. Canada (Global Affairs)* 2024 FC 88

4 *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403; *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8.

Date modified: