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

Access to Information Act: Plain Language Guide to Exemptions and Exclusions / Privacy Act: Plain Language Guide to Exemptions and Exclusions

Published: 2023-09-25

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

Catalogue Number: BT39-78/2023E-PDF
ISBN: 978-0-660-67889-4

This document is available on the Government of Canada website at www.canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Un guide en langage clair et simple sur les exceptions et exclusions prévues par la Loi sur l’accès à l’information / Un guide en langage clair et simple sur les exceptions et exclusions prévues par la Loi sur la protection des renseignements personnels

Access to Information Act: Plain Language Guide to Exemptions and Exclusions

On this page

Introduction

This guide is for people who want more information on the exemptions and exclusions to Access to Information and Privacy (ATIP) requests. It will help them understand why some of the information they requested has been redacted or not released.

The guide is organized by the sections of the *Access to Information Act* (ATIA) that deal with exemptions and exclusions.

Exemptions

Sections 13 to 26 of the ATIA deal with exemptions. Exemptions limit access to information. This could be because the information could cause injury to a person or the country if released. Or it could be because of how the information was obtained (such as during an investigation).

For more information on exemptions, refer to Appendix C of the *Directive on Access to Information Requests*.

Exclusions

Sections 68 and 69 of the ATIA outline information that is not subject to, and cannot be released under the ATIA. These sections are referred to as exclusions.

For more general information on exclusions, including specific documents that are protected, refer to chapter 13 of the *Access to Information Manual*.

Severing non-protected information from protected information

According to section 25 of the ATIA, institutions must still release any part of a record that does not contain protected information and that can be severed, or separated, from the protected information.

For example, a person requests information, and some of that information is protected. But that means that only part of the record cannot be released. The institution must release the rest of the information that is not protected. If the first sentence of a paragraph contains information protected under the *Access to Information Act,* but the rest of the paragraph does not, only the first sentence of the record should be redacted.

Section 13: Information obtained in confidence

The Government of Canada works with other governments, as well as international governmental organizations such as the United Nations. As part of this work, the Government of Canada may obtain confidential information from a governmental source that is protected under section 13.

Rationale

Section 13 protects information that the federal government obtains in confidence from other governments or organizations. Section 13 gives assurance to governments or other organizations that the Government of Canada will not release information provided in confidence.

Description

Subsection 13(1) protects confidential information supplied by other governments or international organizations of states. According to this subsection, the head of a Government of Canada institution must refuse to release information obtained in confidence from:

a. the government of a foreign state or one of its institutions
b. an international organization of states or one of its institutions
c. the government of a province or one of its institutions
d. a municipal or regional government or one of its institutions that was established under an act of the legislature of a province
e. an aboriginal government as specified in subsection 13(3)

There may be two exceptions to this section:

1. where the entity who supplied the information agrees to release the information

2. where the source of the information makes that information public

Section 14: Federal–provincial affairs

The Government of Canada works with provinces and territories and other organizations on federal–provincial issues to ensure smooth government operations across the country.

The *Access to Information Act* (ATIA) allows federal government departments to protect information that would harm the Government of Canada's ability to conduct these activities.

Rationale

The Government of Canada's work with provincial partners is vital to ensuring that governments across Canada function properly.

For this work, the Government of Canada may gather or prepare sensitive information. The Government of Canada's ability to do this work could be harmed if this sensitive information were released.

Description

Section 14 allows the head of a government institution to refuse to release information that could harm the Government of Canada's ability to conduct federal–provincial affairs.

Information that could be withheld under this section includes, but is not limited to:

a. federal–provincial consultations or deliberations
b. strategies or tactics adopted or to be adopted by the Government of Canada about federal–provincial affairs

Section 15: International affairs and defence

The Government of Canada works to ensure the safety of Canadians and advance Canada's interests abroad.

Some government institutions deal with security threats, such as cyberattacks and terrorist activities. Other institutions have a diplomatic role, or play a role in military or other defence activities.

To advance these international interests, the Government of Canada may work with and share information with other countries and international organizations. Releasing this sensitive information to the public may harm the government and its allies ability to do this work.

Rationale

Government institutions that work abroad and conduct global and national security operations must protect the sources and methods required to do their jobs.

Revealing frank views and assessments of foreign government's situations or capabilities may harm diplomatic relations with that country. Revealing an intelligence source publicly could compromise the flow of valuable information and the source's safety.

The release of this kind of information can make it more difficult for the Government of Canada to detect threats to the country.

Description

Section 15 allows the head of a government institution to refuse to release information if the release could harm:

- the conduct of international affairs
- the defence of Canada or any state allied with Canada

- the detection, prevention or suppression of subversive or hostile activities such as espionage or sabotage

For other examples, refer to the *Access to Information Act*, section 15.

Subsection 16(1): Law enforcement and investigations

Many Government of Canada institutions enforce laws that ensure the safety of Canada and Canadians.

Law enforcement often refers to policing. However, Canada also enforces laws relating to administrative matters, such as tax enforcement. Enforcing these laws usually requires conducting investigations. Investigations typically create or collect a wide range of information.

Some information is collected through specialized policing techniques. These techniques are usually kept confidential to protect the investigative process. The *Access to Information Act* (ATIA) allows government institutions to protect information that may make it difficult for them to conduct lawful investigations if it were released.

Rationale

Publicly releasing information about law enforcement activities or investigations could make it more difficult for Government of Canada institutions to enforce laws or carry out important functions such as protecting national security. It could interfere with criminal or other investigations or prosecutions. It could reveal techniques used to gather and analyze evidence. It could hurt relationships with confidential information sources. It could even make it difficult to make arrests by allowing people or organizations to evade law enforcement officials.

Description

Subsection 16(1) states that the head of a government institution may refuse to release a record that contains, for example:

- information obtained or prepared by a government institution that conducts investigations
- information relating to investigative techniques or plans for specific lawful investigations
- information that, if released, could harm the enforcement of any law of Canada or a province or the conduct of lawful investigations
- information that, if released, could harm the security of penal institutions

Subsection 16(2): Security

The Government of Canada is responsible for protecting the safety and well-being of Canadians.

When a government institution produces or obtains information that could make it easier for someone to commit a crime, the head of the institution may protect this information from release.

For example, if a criminal investigation conducted by the Government of Canada revealed the security vulnerabilities of a public or private institution, the information could be protected under subsection 16(2) so that it cannot be used to commit a crime.

Rationale

Releasing information that could make it easier to commit a crime could harm the security of Canadians. A government institution can refuse to release information if it believes that releasing the requested information

would make it easier to commit a crime.

While most of this information could be protected under subsection 16(1), subsection 16(2) makes it easier to process requests for this type of information.

Description

Subsection 16(2) states that the head of a government institution may refuse to release any record that contains information that could make it easier to commit a crime. For example, this can include information:

- on criminal methods or techniques
- about weapons or potential weapons
- on the vulnerability of buildings or other structures or systems, or methods to protect such buildings or other structures or systems

Subsection 16(3): Policing services for provinces or municipalities

The Royal Canadian Mounted Police (RCMP) is Canada's national police force. The RCMP often performs policing services for provincial and municipal governments.

Subsection 16(3) of the *Access to Information Act* (ATIA) states that a government institution will refuse to release any record that contains information that the RCMP obtained or prepared while performing policing services for a province or a municipality in situations where the federal government has agreed with a request from the province or municipality to not release the information.

Rationale

The RCMP gathers information while performing policing services for provinces or municipalities.

Subsection 16(3) allows provincial and municipal authorities to get the federal government's cooperation to protect the information that the RCMP obtained or prepared in relation to policing services in their jurisdiction.

For example, if the RCMP provided policing services to a municipality in relation to organized crime, the municipality may want to protect that information because it relates to future investigations or pending litigation.

Description

Subsection 16(3) states that the head of a government institution will not release any record that contains information that was obtained or prepared by the RCMP while performing policing services for a province or municipality.

Sections 16.1(1) and 16.1(2): Investigations, examinations and audits

Subsection 16.1(1) protects information about investigations, for example, how they are conducted. Section 16.1 protects information obtained or prepared during an investigation, examination or audit by or for the following institutions:

- the Auditor General
- the Commissioner of Official Languages
- the Information Commissioner
- the Privacy Commissioner

Subsection 16.1(2) states once any proceeding related to the audit or investigation is over, neither the Privacy or Information Commissioner cannot refuse to release information created by them or on their behalf under 16.1(1).

Rationale

Releasing information regarding an open investigation may harm the integrity and outcome of the investigation. Protecting this information also protects these institutions ability to perform their other duties and powers.

Description

Subsection 16.1(1) states that the following heads of government institutions will refuse to release any record that contains information that was obtained or created by or for them during an investigation, examination or audit conducted by them or under their authority:

- the Auditor General of Canada
- the Commissioner of Official Languages for Canada
- the Information Commissioner
- the Privacy Commissioner

Section 16.2: Records relating to investigations

The Commissioner of Lobbying ensures transparent and ethical lobbying by administering the *Lobbying Act* and the *Lobbyists Code of Conduct*.

To protect the people involved and the integrity of the investigation, the *Access to Information Act* (ATIA) allows the Commissioner of Lobbying to protect information about investigations. Only the Commissioner of

Lobbying may apply subsection 16.2.

Rationale

Releasing information regarding an open investigation may harm the integrity and outcome of the investigation.

Information obtained or created by the Office of the Lobbying Commissioner about an investigation may include harmful information, particularly towards a lobbyist organization.

For example, if a lobbyist organization was accused of breaching protocol, it may harm their reputation and business in the future.

Description

Subsection 16.2 states that the Commissioner of Lobbying will refuse to release any record that contains information that was obtained or created by the Commissioner or on the Commissioner's behalf in the course of an investigation.

Section 16.3: Investigations, examinations and reviews under the *Canada Elections Act*

The Chief Electoral Officer's primary task is to administer elections, referendums and other aspects of the federal electoral system as described in the *Canada Elections Act*.

To protect the integrity of investigations performed under the authority of the *Canada Elections Act*, the *Access to Information Act* (ATIA) allows the Chief Electoral Officer to protect information about investigations.

Rationale

Releasing information regarding an open investigation may harm the integrity and outcome of the investigation.

Information obtained or created by the Chief Electoral Officer about an investigation may include sensitive information.

For example, if the Chief Information Officer was to investigate malpractice of a political organization, it may cause reputational damage.

Description

Subsection 16.3 states that subject to section 541 of the *Canada Elections Act,* the Chief Electoral Officer will refuse to release any record that contains information that was obtained or created by a person who conducts an investigation under the *Canada Elections Act*.

Section 16.4: Public Sector Integrity Commissioner

The Public Sector Integrity Commissioner investigates wrongdoing in the federal public service and helps protect whistleblowers.

To protect people who contact the Public Sector Integrity Commissioner about alleged wrongdoing, the *Access to Information Act* (ATIA) allows the Office of the Integrity Commissioner to protect information about investigations.

Rationale

Information obtained or created by the Office of the Integrity Commissioner about an investigation may include sensitive or harmful information, particularly towards a whistleblower.

For example, if a whistleblower contacted the Public Sector Integrity Commissioner with damaging information about practices or negligence by a Government of Canada institution and that information became public, the whistleblower may be vulnerable to reprisals.

Description

Subsection 16.4(1) states that the Public Sector Integrity Commissioner will refuse to release any record that contains information:

a. obtained or created by or for them during an investigation under the *Public Servants Disclosure Protection Act*
b. received by a conciliator while trying to reach a settlement of under the *Public Servants Disclosure Protection Act*

Section 16.5: *Public Servants Disclosure Protection Act*

The *Public Servants Disclosure Protection Act* allows federal public servants to report allegations of wrongdoing in their workplace safely and confidentially.

Both the allegations and any potential investigations are often sensitive. The *Access to Information Act* (ATIA) requires that heads of government institutions protect that information.

Rationale

The purpose of this exemption is to allow federal public servants to safely report allegations of wrongdoing in the workplace. Section 16.5 protects the entire investigative process.

The ability to report wrongdoings safely not only helps ensure the integrity of the public service, but also protects those who release wrongdoing.

Description

Section 16.5 states that the heads of government institutions will refuse to release any record requested under Part 1 of the ATIA that contains information created:

- to make a release under the *Public Servants Disclosure Protection Act*
- during an investigation into a release under the *Public Servants Disclosure Protection Act*

Section 16.6: Secretariat of National Security and Intelligence Committee of Parliamentarians

The National Security and Intelligence Committee of Parliamentarians (NSICOP) has a mandate to review the legislative, regulatory, policy, administrative and financial framework for Canada's national security and intelligence community. The Secretariat of the National Security and Intelligence Committee of Parliamentarians (the Secretariat) helps NSICOP fulfill its mandate.

NSICOP prepares reports for the Prime Minister and Parliament with sensitive information redacted.

To draft these reports, NSICOP can access any information, with few exceptions, that is under the control of a government institution. This means that the Secretariat may obtain or create highly sensitive records about national security and intelligence.

The *Access to Information Act* (ATIA) states that the Secretariat must protect this information from being released.

Rationale

NSICOP members hold the highest level of security clearance and are bound to secrecy by the *Security of Information Act*. This allows them to receive classified briefings and access sensitive materials to review Canada's national security and intelligence organizations.

The Secretariat supports NSICOP in performing their reviews. This organization is made up of public servants who can also access sensitive materials but, unlike NSICOP, the Secretariat is subject to the ATIA.

To protect national security and intelligence interests, section 16.6 protects all materials obtained or created by the Secretariat in support of NSICOP's mandate from being released.

Description

Section 16.6 states that the Secretariat must refuse to release any record that contains information obtained or created by or for it while assisting the NSICOP in fulfilling its mandate.

Section 17: Safety of individuals

Sometimes, the Government of Canada has or learns of information that could put individuals in danger if that information were released.

When the information being requested could put individuals in danger, the *Access to Information Act* allows the government to protect that information from being released.

Rationale

This exemption protects individuals against physical or psychological harm. It does not protect an individual's economic security. The risk to the individual must be serious.

The risk is based on many factors, including past threats made against an individual and the behaviour of the potential offender.

Description

Section 17 states that the head of government institutions may refuse to release any record requested if they have reasonable grounds to believe that the release of the information could threaten the safety of an individual.

Section 18: Economic interests of Canada

Many government institutions support the Canadian economy.

For instance, the Bank of Canada sets interest rates. Many Crown corporations (corporations wholly or partly owned by the government, such as Canada Post) provide services to the public. They often generate revenue from those services.

As a result, government institutions hold information about the Government of Canada's, or specific institutions' economic interests. The *Access to Information Act* (ATIA) allows the government to protect some of this information when it has substantial value, or if releasing it would harm the government's business interests or its competitive position.

Rationale

The Government of Canada actively manages the Canadian economy to ensure that it is stable. The government provides services or develops research through Crown corporations and other institutions. The government also procures services. All these activities create information that should be protected.

For instance, if a government institution were to tell a company that was bidding on a government contract what the maximum value of the contract is, that would drive up the bids. If an institution releases information used to create patented technology, it could have difficulty earning revenue from that patent.

Description

Section 18 allows the head of a government institution to withhold information that is in the economic interest of Canada.

Examples of this type of information include:

- Trade secrets, meaning a plan, process, tool, mechanism or compound that belongs to the Government of Canada or a government institution. Examples include a vaccine formula, a recipe, or an exclusive technological process
- Financial, commercial, scientific or technical information. To qualify, a record must contain these types of information and cannot be protected only because it was created in the context of financial or commercial work
- Information that, if released, could injure the financial interests of a government institution or interfere with the Government of Canada's ability to manage the economy, or result in an undue benefit to any person, including information about:

i. Canadian currency or coinage
ii. a contemplated change in the bank interest rate or government borrowing
iii. a contemplated change in tariff rates, taxes, duties or any other revenue source
iv. a contemplated change in the conditions under which financial institutions operate
v. a contemplated sale or purchase of securities or of foreign or Canadian currency
vi. a contemplated sale or acquisition of property

Subsection 18.1(1) allows the head of a government institution to refuse to release a record that contains trade secrets or financial, commercial, scientific or technical information that belongs to, and has been consistently treated as confidential by:

- the Canada Post Corporation
- Export Development Canada
- the Public Sector Pension Investment Board
- Via Rail Canada Inc.

There are two exceptions to the ability to withhold information under this section:

1. if the information is related to the general administration of these four institutions
2. if the information is related to activities at Canada Post Corporation that are fully funded by Parliament

Section 3.1 explains “general administration” as information that relates to the expenses paid by the institution including for travel, lodging and hospitality.

Section 19: Personal information

Everyday, people provide the Government of Canada with their personal information for a variety of reasons, including:

- to obtain benefits, such as disability benefits
- to complete their income and dependent information in a tax return
- to complete surveys and statistical reports, and procure services that may result in personal information being recorded, such as a person's age, race, ethnic background or religion

Any information that is recorded about an identifiable individual is considered "personal information." It must be appropriately safeguarded, used and managed in accordance with the *Privacy Act*.

Rationale

For the Government of Canada to provide effective services, it often must collect personal information from individuals. Those individuals need to trust the government will use that information responsibly and in accordance with the *Privacy Act*.

The Government of Canada may release personal information in specific instances:

- an individual has a right to obtain their own personal information through a request under the *Privacy Act*
- information that is already publicly available may be released
- the individual can consent to release their personal information

Section 8 of the *Privacy Act* permits information to be released under other circumstances.

Description

Subsection 19(1) protects personal information in records held by government institutions.

Except in very specific circumstances, subsection 19(1) requires the head of a government institution to withhold personal information. Information must meet the following three requirements to be defined as personal information:

1. The information is about an identifiable individual. The name of the individual is in the record, or the identity of the individual can be deduced by the information in the record, whether alone or when combined with information from other sources.
2. The information is about an individual. Information about corporations and other legal persons does not fall within the definition of personal information. However, information about individual(s) in a sole proprietorship or in a partnership would be considered “personal information” within the meaning of section 3 of the *Privacy Act*.
3. The information is recorded. It can be recorded in any form. For example, video recordings and photographic images of individuals contain personal information about them because they show something about their race, gender, age and ethnic origin, as well as their appearance or the sound of their voice. This applies to recordings and images of employees of a government institution and public figures. Oral conversations, even if personal in nature, are not considered personal information for the purposes of the *Privacy Act*, unless the conversation is recorded in some manner.

There are three situations where this type of personal information may be released:

1. where consent is obtained from the individual

2. where the information is publicly available
3. where the release is allowed under section 8 of the *Privacy Act*

Section 20: Third-party information

The Government of Canada interacts with private businesses every day for many reasons.

These businesses, as well as non-government organizations, charities and not-for-profit organizations, are known within government as “third-party organizations.” The information shared by these organizations may include trade secrets or other confidential business information.

Rationale

Third-party organizations share information with the government. Some are required to, for example to ensure that they are complying with regulations. Others voluntarily share information, such as when a company bids on a government contract.

That information can become subject to the *Access to Information Act* (ATIA). There are certain types of information that third-party organizations share that may need to be protected. Each situation is assessed on a case-by-case basis.

There are many factors that affect whether information must be released, including:

- why the information was provided to the government, and any obligations around those circumstances
- whether the information is already publicly available, for example a published corporate report

- whether the information was provided to the government in confidence and has been consistently kept confidential
- if the third party agrees to release the information

The government must not release the following types of third-party information. Once information falls into one of the categories set out in paragraphs 20(1)(a), 20(1)(b), 20(1)(b.1), 20(1)(c), or 20(1)(d) of the ATIA, it must be protected.

Trade secrets of a third party 20(1)(a)

The term “trade secret” has a traditional legal meaning, that of a plan, process, tool, mechanism, or compound that is known by a relatively small number of people. A few examples of a trade secret include a vaccine formula, a recipe, or an exclusive technological process used by a manufacturer that provides the third party with a commercial or competitive advantage.

Financial, commercial, scientific or technical information 20(1)(b)

This information should not be available online or obvious to an observer. It should be expected that the information will be confidential when it is created. The information needs to have been supplied by the third party in confidence to the government, and consistently treated as confidential by the third party. Examples of confidential third-party information include market strategies or details about a manufacturing assembly line.

Information supplied in confidence to a government institution concerning emergency management plans 20(1)(b.1)

This sub-category refers specifically to information supplied by a third party in confidence to a government institution about critical infrastructure to allow the institution to prepare, maintain, test or implement emergency

management plans.

This exemption protects information about vulnerabilities in a third party's buildings, networks or systems, and measures taken to protect against those vulnerabilities. This includes assessments of the security of cyber systems, the location of vaccine stockpiles, or maps of facilities.

Material financial loss, gain or prejudice 20(1)(c)

This category includes information that may harm a company's competitive position, either by describing that company's practices, or by making it difficult for the company to make money.

For example, if the information can provide competitors with a clear picture of a company's costs to complete certain work, competitors could undercut them in bidding for government contracts.

Interference with contractual or other negotiations 20(1)(d)

This category includes information about a third party's involvement in negotiations. The release of this information may obstruct those negotiations.

An example is information that would reveal a third party's position during negotiations. If released, this information could negatively affect the outcome of the negotiations.

Public interest override (20(6))

In certain circumstances, some third-party information is not protected under the *Access to Information Act*, even if the information would normally be protected.

These circumstances include a clear public health, safety or environmental concern. Information may also be released if the public interest is greater than any financial loss or gain, or any concern to the security of structures, networks or systems, competitive position or contractual obligations.

This override does not apply to trade secrets. The rights of third parties must be carefully weighed against the general public's rights to safety, while balancing Canada's need for competitive and innovative business markets.

Description

Subsection 20(1) requires the head of an institution to refuse to release records that contain the following types of third-party information:

- trade secrets
- confidential financial, commercial, scientific or technical information
- confidential information used for emergency management plans (preparation or testing of plans)
- information that, if released, could reasonably be expected to harm the competitive position of a third party, or result in material financial loss or gain
- information that, if released, could interfere with a third party's contractual or other negotiations

The government institution may be able to release information if the third-party consents or if it would be in the public's interest. The public interest must also be clearly more important than the financial loss, prejudice to the security of the third party's infrastructure, competitive position or interference with its contractual negotiations.

Government institutions will sometimes extend the deadline to respond to a request to seek the third party's agreement to release their information.

Section 20.1: Public Sector Pension Investment Board

The Public Sector Pension Investment Board (PSPIB) is a Canadian Crown corporation. PSPIB is the pension investment manager for the federal public service, Canadian Armed Forces, RCMP and the Reserve Force.

In exercising their mandate, PSPIB may hold investment advice or information obtained in confidence from third parties. If the PSPIB has consistently kept the information confidential, the *Access to Information Act* (ATIA) protects this information from release.

Rationale

Some types of information shared with the government can be sensitive, and the government must assume that injury will result from releasing the information. Once information is determined to be sensitive, this is enough reason to protect the information.

This is the case for the type of information set out in section 20.1: advice or information relating to investments obtained by PSPIB in confidence from a third party and which they have consistently treated as confidential.

PSPIB must be able to seek advice and obtain information from third parties in confidence to grow their investments. If PSPIB were required to release advice or information obtained in confidence, other parties could gain a competitive advantage over PSPIB.

Description

Section 20.1 can be invoked only by the PSPIB or wholly owned subsidiaries. It states that the head of the PSPIB shall refuse to release a record that contains advice or information obtained in confidence from a third party,

such as confidential financial statements, so long as the PSPIB has consistently treated the advice or information as confidential.

Section 20.2: Canada Pension Plan Investment Board

The Canada Pension Plan Investment Board (CPPIB) is a Canadian Crown corporation. The CPPIB is the pension investment manager for the Canada Pension Plan Fund, which is available to members of the Canadian public.

In exercising their mandate, the CPPIB may hold investment advice or information obtained in confidence from third parties. If the CPPIB has consistently kept the information confidential, the *Access to Information Act* (ATIA) protects this information from release.

Rationale

Some types of information shared with the government can be sensitive, and the government must assume that injury will result from releasing the information. Once information is determined to be sensitive, this is enough reason to protect the information.

This is the case for the type of information set out in section 20.2: advice or information relating to investments obtained by CPPIB in confidence from a third party and which they have consistently treated as confidential.

The CPPIB must be able to seek advice and obtain information from third parties in confidence to support the growth of their investments. If the CPPIB released advice or information obtained in confidence, then other parties could gain a competitive advantage over the CPPIB.

The CPPIB has the same protection under the ATIA as any private sector investment firm operating in the same environment.

Description

Section 20.2 can be invoked only by the CPPIB and its wholly owned subsidiaries. It states that the head of the CPPIB shall refuse to release a record requested that contains advice or information relating to investment the CPPIB obtained in confidence from a third party if the CPPIB has consistently treated the advice or information as confidential.

Section 20.4: National Arts Centre Corporation

The National Arts Centre (NAC) Corporation is a Canadian Crown corporation. The NAC Corporation's mandate is to:

- operate and maintain the NAC
- develop the performing arts in the National Capital Region
- help the Canada Council for the Arts develop performing arts elsewhere in Canada

To fulfill their mandate, the NAC hires performing artists to perform at the NAC and manages charitable donations to sustain its programs. As a result, the NAC holds information about the contracts for performing artists and the identities of donors.

The *Access to Information Act* (ATIA) requires the NAC to protect information about performing artists and donors if the NAC has consistently treated the information in a confidential manner.

Rationale

The NAC works in the highly competitive field of performing arts.

The ATIA does not protect all contractual information of a performing artist, such as the administration of the contract, but it does cover specific terms, including the description of the work and conditions of payment. The ATIA allows the NAC to protect contractual terms in the same way a private venue would.

The identity of a donor who donated in confidence is private information. The ATIA does not protect all of the information about the donation, for example, the amount or purpose. If the donor is an individual, the *Privacy Act* would protect information about donations made in confidence under personal information. The ATIA ensures that this protection applies to both private citizens and private organizations who donate to the NAC in confidence.

Description

Section 20.4 states that the head of the NAC or its wholly owned subsidiaries will not release a record if the release would reveal the terms of a contract for the services of a performing artist or the identity of a donor who has made a donation in confidence if the NAC has consistently treated the information as confidential.

Section 21: Operations of government

The Government of Canada develops policies and makes decisions on government spending, programs, and activities. The *Access to Information Act* (ATIA) makes it easier for the public to learn about decision-making and government operations.

However, when government programs or policies are under development, a high degree of public attention can influence the decision-making process.

To choose the best course of action, government analysts must review all possible options, including those that may seem unlikely or that may have unintended or negative outcomes. Until the government or a delegated official makes a decision, none of the options represent official government positions.

If people were to mistake these options for official government positions, it could make it difficult for the government to govern effectively. It could also limit options and advice in the future. Government employees may be more focused on public perception than on providing their objective views to government decision-makers.

Officials who advise decision-makers must be able to give their full and free advice on options being considered for public policy, priorities or programming decisions. The public is best served by the best plans, considering all policy options and negotiating the best deals. All of these require a degree of confidentiality in their development and execution.

Rationale

The ATIA requires that heads of institutions must weigh the risks and benefits of releasing information.

For instance, once a negotiation is concluded, the materials prepared to plan the negotiation may be less sensitive. Similarly, once a policy decision has been made, the options that were not adopted may also no longer be sensitive. Some other factors that the Federal Court has raised include:

- the age of the information
- whether the information could be found through public means, including by observation
- whether the information was developed with a reasonable expectation of confidentiality

- whether the release of this information would hurt future processes
- the degree and type of public attention on a particular issue (e.g. press coverage)
- whether parts of the information could be separated and released without losing important context

In addition to the general descriptions above, there are some specific considerations in this exemption in the ATIA.

Advice or recommendations 21(1)(a)

This exemption protects information where there is a clear proposed course of action, such as recommendations and advice. It does not apply to background or factual information such as statistics.

When the Government of Canada adopts a recommendation, it becomes public policy and is no longer subject to this exemption. Paragraph 21(1)(a) also protects options that were not taken, though the head of the institution must consider whether that information is still sensitive.

Account of consultations or deliberations 21(1)(b)

This exemption protects the record of a discussion where multiple government officials are considering or debating the merits of one or more courses of action. The same considerations for paragraph 21(1)(a) apply for this paragraph.

Positions or plans developed for negotiations 21(1)(c)

This exemption protects positions or plans developed for negotiations by or for the federal government. Unlike paragraphs (a) and (b), paragraph 21(1)(c) may protect background information that could reveal the Government

of Canada's positions. However, after the conclusion of negotiations, the information may no longer be sensitive.

Management or personnel plans 21(1)(d)

This paragraph protects staffing or administrative planning by a government institution. As with paragraph (c), background information that would reveal sensitive information about those plans may be protected. But, paragraph 21(1)(d) notes that once a plan is implemented, it is no longer subject to this exemption.

Subsection 21(2) Exceptions

Two general exceptions prevent the use of subsection 21(1):

a. The exercise of any power or function that affects the rights of a person. When the rights of a person might be affected by the decisions of another, the reasons for that decision must be available to the affected person.
b. Reports prepared by contractors. Government contractors are not public servants and are not subject to the same laws and regulations as the public service.

Description

Subsection 21(1) of the ATIA states that the head of an institution can refuse to release a record that is less than 20 years old containing information about:

- advice developed by or for the government institution or a minister
- consultations that the government or the Crown participate in
- plans developed for negotiations by the government
- plans on the management of an institution that are not yet operational

Section 22: Testing procedures, tests and audits

Government institutions routinely administer tests to potential candidates and conduct audits of personnel or finances.

As a result, government institutions hold information about specific planned tests and audits, and the procedures or techniques behind them. The *Access to Information Act* (ATIA) allows institutions to protect this information.

Rationale

In certain situations, releasing information about the content, procedures or techniques behind tests and audits conducted by a government institution could provide an unfair advantage to an individual or entity who is the subject of that test or audit.

Protecting this information means government institutions can ensure that tests or audits are fair.

Description

Section 22 states that the head of a government institution may refuse to release information about testing, auditing procedures, techniques and details of specific tests to be given or audits to be conducted.

Subsection 22.1(1): Internal audits

Government institutions audit their internal programs to evaluate program effectiveness. The internal audit process produces both working papers (planning documents, questionnaires, notes from interviews) and draft

reports. The *Access to Information Act* (ATIA) allows the government to protect these working papers and draft reports from release.

Internal audit means a specific professional, independent and objective appraisal that uses a disciplined, evidence-based approach to assess and improve the effectiveness of risks management, control and governance processes.

Subsection 22.1(1) is time-limited and cannot be applied to records for internal audits that are more than 15 years old at the time of the request.

Subsection 22.1(2) Exceptions

There are two exceptions to the use of subsection 22.1(1):

a. Releasing a draft report of an internal audit of a government institution when a final report of the audit has been published
b. The institution has not received a final report of the audit within two years after the day on which the audit began

Rationale

If working papers or draft reports of an internal audit are released early, it may interfere with both an ongoing evaluation and the conclusions in the final report.

Releasing a draft report could harm the integrity of the objective audit process. In an ongoing evaluation, some details and the conclusions in the draft report may be different from those found in the final report.

This section of the ATIA gives the subject of an audit the chance to review and respond to conclusions in the draft report. The final report also generally includes a management response. It is in the public's best

interest for this information to be protected to allow thorough and objective audits of government programs.

The time limit allows the public to access internal audit records after access would no longer compromise the integrity of the audit.

Description

Subsection 22.1(1) states that the head of a government institution may refuse to release any record containing a draft report of an internal audit of a government institution or any related audit working paper if the record came into existence less than 15 years before the request.

Section 23: Solicitors, advocates and notaries

Government institutions administer and adhere to laws as part of their regular business.

Institutions must act within their legal authority, and sometimes their decisions or actions can be challenged before the courts. As a result, government institutions frequently employ legal professionals to advise and support them.

Institutions hold information about these activities, such as legal opinions, routine communications, and court filings. The *Access to Information Act* (ATIA) allows the government to protect some of this information when it is subject to solicitor–client privilege.

The solicitor–client privilege exemption refers to two types of privilege: solicitor–client privilege and litigation privilege.

- Solicitor–client privilege, also known as legal advice privilege, applies to all communications, between a lawyer and their client. Solicitor-client privilege does not apply to political, administrative, managerial or general policy advice.
- Litigation privilege applies to records created for ongoing or anticipated litigation.

Rationale

Solicitor–client privilege is necessary to administer justice and maintain the public's confidence in the legal system.

Solicitor–client privilege allows clients and their legal professionals to have candid discussions. Clients need to be assured that communications between them and their legal representatives are strictly confidential. This privilege never expires.

Litigation privilege allows litigators to prepare their cases in private without interference by the other party before they make their case in court.

Section 23 ensures that government institutions receive the same protections for communications with their legal professionals, similar to the private sector.

Section 23 does not apply where solicitor–client privilege has been waived.

Description

Section 23 states that the head of a government institution may refuse to release any record containing information subject to solicitor–client privilege.

Section 23.1: Protected information – patents and trademarks

Patents protect inventions, processes, and scientific creations from being copied. Likewise, trademarks protect brands, logos, and slogans from being copied.

Patent agents and trademark agents are licensed professionals that help clients secure legal protections for their intellectual property by submitting patent or trademark applications.

Subsection 23.1 of the *Access to Information Act* (ATIA) protects privileged communications between clients and their patent or trademark agent.

Rationale

Conversations between patent agents or trademarks agents and their clients may involve sensitive information regarding intellectual property and are privileged in the same way as solicitor-client privilege.

If sensitive information regarding intellectual property was made public, a competitor may use that information to their advantage.

Description

Subsection 23.1 states the head of an institution may refuse to release a record that contains information subject to privileges set out in section 16.1 of the *Patent Act* or section 51.13 of the *Trademarks Act*.

Section 24: Statutory prohibitions against release

The Government of Canada administers many laws. In certain cases, these laws prevent the release of certain information under the *Access to Information Act* (ATIA).

For example, the *Canadian Navigable Waters Act* prevents the release of Indigenous knowledge provided to the government in confidence. The *Statistics Act* protects responses to surveys by identifiable individuals. Schedule II of the ATIA lists laws and their provisions that restrict the release of certain information.

If the law that prevents release under the ATIA offers an alternative method for accessing the information, the institution should inform the requestor.

If the law that prevents release under the ATIA does not offer an alternative method for accessing the information, but does allow specific information to be released with the consent of the party involved, the institution should inform the requestor.

Rationale

This section ensures that the ATIA is aligned with other Canadian laws and prevents information that is otherwise restricted from being released under the ATIA.

Some of the laws listed in Schedule II of the ATIA will provide an alternative method for accessing information, outside of the ATIA. For example, the *Statistics Act* allows the Chief Statistician to release information with the written consent of the person or organization concerned.

Some laws do not have alternative methods, but allow information to be released under certain conditions, such as if the party involved agrees to release it. In those cases, the institution processing the ATIA request needs to seek consent.

Description

Subsection 24(1) states that the head of a government institution will not release any record that contains information that is restricted by or under any provision set out in Schedule II.

Section 26: Refusal of access if information to be published

The Government of Canada publishes many types of information, such as reports to Parliament, manuals and studies. These products are used by members of the public for many reasons, so they should be made available to both the government and the public at the same time.

The *Access to Information Act* (ATIA) protects information that will become publicly available within 90 calendar days to ensure that the public and Parliament are treated fairly and can view the material at the same.

Rationale

There are several reasons why the Government of Canada may withhold information that has not yet been published, but soon will be:

- to ensure that certain information that must be published in the public interest will be made available to everyone at the same time in both official languages

- to allow time for some government publications to pass through other review processes, such as scientific studies that are peer-reviewed

Description

Section 26 states that a government institution may refuse to release a record if the head of the institution believes that the material will be published within 90 days after the request is made, or as soon as possible after translating or printing the material.

Section 68: Published material, material available for purchase, and museum material

The Government of Canada publishes many types of information. Government institutions also have information that is for sale to the public, such as subscription-based newspapers or journal articles.

Federal museums and libraries preserve certain information to exhibit or for the public's use. They also accept donations of materials by the public, private organizations or representatives acting on their behalf.

The *Access to Information Act* (ATIA) excludes published information, except for the material listed in Part 2 of the ATIA. Also excluded are materials that can be purchased, that are preserved in a museum or library for public reference or exhibition, or that are donated to museums by private individuals or organizations.

Rationale

Published material is excluded to save the government time and effort collecting material that can be accessed by the public in other ways. For example, laws can be accessed through the Department of Justice Canada website, and official communications are often published via social media.

Material available for purchase by the public is excluded to protect the copyright owners, for example newspaper columnists or academics. This means that the public cannot use the ATIA to obtain material for less than the purchase price.

Museums and libraries preserve material for public reference and exhibition purposes. This includes material donated by private citizens or organizations. This material is protected to prevent the public from accessing the material held by museums or libraries for the cost of the ATIA application fee instead of paying for the services of the museum or library.

This exclusion has one exception. Material published by institutions under Part 2 of the ATIA is protected. Section 68 does not apply to these publications.

Description

Section 68 is an exclusion that states that Part 1 does not apply to the following categories of information:

- published material, other than material published under Part 2 or material available for purchase by the public
- library or museum material preserved solely for public reference or exhibition purposes
- material placed by or on behalf of persons or organizations other than government institutions in the:
    - Library and Archives of Canada

- National Gallery of Canada
- Canadian Museum of History
- Canadian Museum of Nature
- Canada Science and Technology Museum
- Canadian Museum for Human Rights
- Canadian Museum of Immigration at Pier 21

Individuals who make a request under Part 1 of the ATIA have a right to complain to the Information Commissioner and seek review by the Federal Court.

Section 68.1: Canadian Broadcasting Corporation

The Canadian Broadcasting Corporation (CBC) is a Canadian Crown corporation and Canada's national public broadcaster.

It holds information about its administrative activities, such as expenditures and staffing, and about their journalistic, creative and programming activities. Examples of these activities include planned stories, the names of key sources and anticipated programming.

The CBC operates at arm's length from the rest of the Government of Canada but is still subject to the *Access to Information Act* (ATIA). The ATIA excludes information that relates to the CBC's journalistic or creative activities, other than general administration.

Rationale

Freedom of the press is in the *Canadian Charter of Rights and Freedoms*. A free press is important because it means that broadcasters can publish stories without political or public scrutiny or interference.

Since they provide programming other than journalism, broadcasters operate in a competitive environment where each broadcaster wants to attract the most viewers. Releasing planned creative and programming activities could harm a broadcaster's ability to make money from those activities.

Section 68.1 recognizes the unique position of the CBC. They receive government funding, so their management functions and administrative expenditures should be open to public scrutiny. However, the CBC's mandate means that they need the same protections as private broadcasters for their journalistic sources and to maintain their creative and programming independence.

Description

Section 68.1 states that Part 1 of the ATIA does not apply to any information that is under the control of the CBC about its journalistic, creative or programming activities (for example, show or news anchor selection rationale) other than information that relates to its general administration (for example, performance management such as audits or evaluations).

Section 68.2: Atomic Energy of Canada Limited

Atomic Energy of Canada Limited (AECL) is a Canadian Crown corporation. It deals with nuclear science and technology and protects the environment by fulfilling the Government of Canada's radioactive waste and decommissioning responsibilities.

The AECL delivers its mandate through a government-owned, contractor-operated (GoCo) model. A private-sector organization, Canadian Nuclear Laboratories (CNL), manages and operates AECL's sites.

AECL owns the intellectual property resulting from the GoCo model. So, AECL holds information about CNL's research on environmental impacts, health applications of nuclear research and clean energy. AECL also holds information about their commercial activities, such as decommissioning and remediation services.

The AECL operates at arm's length from the rest of the Government of Canada but is still subject to the *Access to Information Act* (ATIA). The ATIA excludes information that relates to the AECL's activities, and that of their wholly owned subsidiaries, other than records related to their general administration and their operation of any nuclear facility.

Rationale

Section 68.2 recognizes that the AECL receives government funding, so their management functions and administrative expenditures should be open to public scrutiny.

However, the ATIA also recognizes that the GoCo model provides AECL with information produced by CNL that relates to CNL's commercial services and work in a sensitive research area.

Releasing information about research and commercial activities could harm CNL's ability to make money from these activities. AECL and CNL should be extended the same protections for their research and commercial activities as private companies.

Description

Subsection 68.2 states that Part 1 of the ATIA does not apply to any information that is under the control of AECL other than information that relates to:

- its general administration

- its operation of any nuclear facility within the meaning of section 2 of the *Nuclear Safety and Control Act* that is subject to regulation by the Canadian Nuclear Safety Commission established under section 8 of the *Nuclear Safety and Control Act*

Section 69: Confidences of the King's Privy Council for Canada

The Canadian government is based on a parliamentary system that includes a Cabinet. The Cabinet is a body of advisors and is a committee of the King's Privy Council for Canada.

Members of the Cabinet are ministers of the Crown who are responsible for all government policy. To set policies and priorities for the country, the Cabinet meets regularly to discuss and make decisions on a variety of issues.

The federal public service provides confidential advice to ministers to support their participation in Cabinet. As a result, institutions hold information about Cabinet meetings and discussions. The *Access to Information Act* (ATIA) excludes these records, as they are confidences of the King's Privy Council.

Rationale

Releasing Cabinet discussions would harm the Cabinet's ability to discuss issues freely and make informed decisions. The decision-making process and its supporting records are traditionally protected, which enables ministers to have open discussions.

Description

Subsection 69(1) states that the ATIA does not apply to confidences of the King's Privy Council for Canada, including:

- memoranda to present proposals or recommendations to council
- discussion papers to present background explanations, analyses of problems or policy options to council for decision-making
- agenda of council or records of council deliberations or decisions
- records used for or reflecting communications or discussions between ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy
- records to brief ministers of the Crown about matters that are before, or are proposed to be brought before, council or that are the subject of communications or discussions referred to in paragraph (d)
- draft legislation
- records that contain information about the contents of any record within a class of records referred to in paragraphs (a) to (f)

Subsection 69(2) specifies that, for the purposes of subsection 69(1), the word "council" means the King's Privy Council for Canada, committees of the King's Privy Council for Canada, Cabinet and committees of Cabinet.

Subsection 69(3) specifies that this exclusion has two exceptions:

- confidences of the King's Privy Council for Canada that are more than 20 years old
- discussion papers (see paragraph 69(1)(b))
    i. if the decisions related to the discussion papers have been made public
    ii. where the decisions have not been made public, if four years have passed since the decisions were made

Section 69.1: Certificate under *Canada Evidence Act*

Certain Government of Canada institutions conduct criminal and civil prosecutions on behalf of the government. These legal proceedings may involve sensitive information obtained in confidence from foreign entities or relating to national defence or national security.

In national security prosecutions, records about the case may contain information on terrorism offences, war crimes, human smuggling, information that is classified or information obtained from foreign law enforcement partners.

The *Canada Evidence Act* (CEA) authorizes the Attorney General of Canada to issue a certificate to prevent sensitive information from being released.

The *Access to Information Act* (ATIA) excludes information that the Attorney General of Canada has issued a certificate about.

Rationale

For the Attorney General of Canada to issue a certificate, there must be a risk to international relations, national defence or national security. Therefore, that information should be excluded from the ATIA.

This section ensures that the ATIA is aligned with the CEA. This means that information that is protected under the CEA cannot be released under the ATIA.

If the Attorney General of Canada issues a certificate after a complaint is filed with the Information Commissioner, the complaint is discontinued. The information cannot be released and must be returned to the institution by the Information Commissioner.

Description

Subsection 69.1(1) states that where a certificate is issued before a complaint is filed under this Part in respect of a request for access to that information, this Part does not apply to that information.

Subsection 69.1(2) states that when a certificate is issued after a complaint is filed under this Part about a request for access to that information:

- all proceedings under this Part in respect of the complaint, including an investigation, appeal or judicial review, are discontinued
- the Information Commissioner shall not release the information and shall take all necessary precautions to prevent its release
- the Information Commissioner shall, within 10 days after the certificate is published in the *Canada Gazette*, return the information to the head of the government institution that controls the information

Date modified:
2023-09-29

Privacy Act: Plain Language Guide to Exemptions and Exclusions

On this page

- Subsection 69(1): Library and museum material
- Section 69.1: Canadian Broadcasting Corporation
- Subsection 70(1): Confidences of the King's Privy Council for Canada
- Section 70.1: Certificate under the *Canada Evidence Act*

Introduction

The *Privacy Act* gives everyone a general right to access their personal information held by government institutions. It also protects that personal information from unauthorized collection, use, retention and disclosure.

However, the right of access to one's personal information has some limits. There are two classes of exceptions to the general right of access:

1. exemptions where certain types of personal information are exempt from the *Privacy Act*'s access requirements
2. exclusions where the *Privacy Act* does not apply to personal information

The *Privacy Act* allows for government institutions to refuse to release certain kinds of personal information. This guide is organized by the sections of the *Privacy Act* that deal with the exemptions and exclusions from release. They will help you understand why parts of your response package have been blacked out and not released to you.

Generally, to be included in the response package, the information must meet the following three requirements to be defined as your personal information and releasable under the *Privacy Act*:

1. You can be identified by the information. Your name is in the record, or your identity can be deduced by the information in the record, whether alone or when combined with information from other sources.
2. The information is about you as an individual. Information about corporations and other legal persons does not fall within the definition

of your personal information. However, information about individual(s) in a sole proprietorship or in a partnership would be considered "personal information" within the meaning of section 3 of the *Privacy Act*.

3. The information is recorded. It can be recorded in any form. For example, video recordings and photographic images of you contain personal information about you because they show something about your race, gender, age and ethnic origin, as well as your appearance or the sound of your voice. This applies to recordings and images of employees of a government institution and public figures. Oral conversations, even if personal in nature, are not considered personal information for the purposes of the *Privacy Act* unless the conversation is recorded in some manner.

Note that when someone gives an opinion or makes a statement about someone else, that opinion or statement is generally considered the personal information of both parties. This can impact whether it is released to you.

Right of access and severability

A personal information request generally gives you access to your own personal information. The records containing your personal information may also include information other than your personal information. Institutions may release some of this additional information to you. In practice, parts of the records that are not exempt or excluded **will not** be blacked out, while the parts of a document where *Privacy Act* exceptions do apply **will be** blacked out.

Exemptions

Sections 18 to 28 of the *Privacy Act* deal with exemptions. These limit one's access to personal information. An exemption could be made, for example, because the release of the personal information could cause injury to a person or the country. It could also be made because of how the information was obtained (such as during an investigation). Some exemptions are mandatory, in which case the institutions are legally required to withhold the personal information. Others are discretionary, in which case privacy officials may decide whether releasing the information is appropriate.

Exclusions

Sections 69 and 70 of the *Privacy Act* are referred to as "exclusions" because they cover information that is excluded from the application of the *Privacy Act*. Individuals do not have a right of access to this information.

Section 18: Exempt banks

Government of Canada institutions collect personal information about individuals for programs or activities, such as granting a benefit or determining how much in taxes is owed. Institutions must publish a listing, called a personal information bank, of the personal information they collect and how it is managed. The listing is published on the institution's Info Source website.

Some personal information banks are for programs and activities focused on international affairs, defence, law enforcement and national security investigations. Given the sensitive nature of personal information that would be held by programs related to these personal information banks, these personal information banks may be designated as exempt from

personal information requests. In such a case, the personal information in these designated banks does not have to be disclosed to the requester under section 18 of the *Privacy Act*. You can find more information about these exempt personal information banks on the institutions' websites.

Rationale

In order to protect its ongoing international affairs, defence, law enforcement and investigations, the Government of Canada does not provide access to the personal information in an exempt bank.

Exempt banks are rare, but they primarily include security, intelligence, national defence, and national security investigation records.

Description

Subsection 18(1) protects exempted personal information banks that contain files predominantly of personal information described in section 21 or 22 of the *Privacy Act*. These sections are also explained in this guide.

Subsection 18(2) allows the head of a government institution to refuse to release personal information contained in an exempt bank under subsection 18(1).

Section 19: Personal information obtained in confidence

The Government of Canada works with other governments, as well as with international governmental organizations such as the United Nations. As part of this work, the Government of Canada may obtain confidential personal information from a governmental source that is protected under section 19.

Rationale

Section 19 protects personal information that the federal government obtains in confidence from other governments or international organizations of states. The section 19 exemption gives assurance to these entities that the Government of Canada will not release information provided in confidence.

Description

Subsection 19(1) protects confidential personal information supplied by other governments or international organizations of states. This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies. The head of a Government of Canada institution must refuse to release personal information obtained in confidence from the following:

a. the government of a foreign state or one of its institutions
b. an international organization of states or one of its institutions
c. the government of a province or one of its institutions
d. a municipal or regional government or one of its institutions that was established under an act of the legislature of a province
e. a First Nations government or council

There may be two exceptions to this section:

1. where the entity who supplied the personal information agrees to release the information
2. where the source of the personal information makes that information public

Section 20: Federal–provincial affairs

The Government of Canada works with provinces and territories and other organizations on federal–provincial issues to ensure smooth government operations across the country.

The *Privacy Act* allows federal government departments to prevent the release of personal information that would harm the Government of Canada's ability to conduct these activities.

Rationale

The Government of Canada's work with provincial partners is vital to ensuring that governments across Canada function properly.

For this work, the Government of Canada may gather and analyze personal information, the disclosure of which could be harmful to the Government of Canada's conduct of federal–provincial affairs. This exemption can be used to prevent the disclosure of personal information judged to be harmful to federal–provincial affairs even if the personal information is not confidential.

Description

As a discretionary exemption, section 20 allows the head of a government institution to refuse to release personal information that could harm the Government of Canada's ability to conduct federal–provincial affairs.

Section 21: International affairs and defence

The Government of Canada works to ensure the safety of Canadians and advance Canada's interests abroad.

Some government institutions deal with security threats, such as cyberattacks and terrorist activities. Other institutions have a diplomatic role or play a role in military or other defence activities.

To advance these international interests, the Government of Canada may work with and share personal information with other countries and international organizations. Releasing this sensitive personal information to the public may harm the government and its allies.

Rationale

Government institutions that work abroad and conduct global and national security operations must protect the sources and methods required to do their jobs.

The personal information of Canadian personnel could reveal sensitive information relating to a military unit or other defence organization, such as the training, capabilities and skills of members. Revealing an intelligence source publicly could compromise the flow of valuable information and the source's safety, even to an individual who previously worked on the file. Finally, protecting opinions expressed about an individual could be important for effective diplomacy.

The release of this kind of personal information can make it more difficult for the Government of Canada to detect threats to the country and its allies.

Description

As a discretionary exemption, section 21 allows the head of a government institution to refuse to release personal information if the release could harm:

- the conduct of international affairs
- the defence of Canada or any state allied with Canada

- the detection, prevention or suppression of subversive or hostile activities such as espionage or sabotage

For further examples, refer to the *Access to Information Act*, section 15.

Subsection 22(1): Law enforcement and investigations

Many Government of Canada institutions enforce laws that ensure the safety of Canada and Canadians.

Law enforcement often refers to policing. However, Canada also enforces laws relating to administrative matters, such as tax enforcement. Enforcing these laws usually requires conducting investigations. Investigations typically create or collect a wide range of personal information.

Some personal information is collected through specialized policing techniques. These techniques are usually kept confidential to protect the investigative process. The *Privacy Act* allows government institutions to protect personal information that may make it difficult for them to conduct lawful investigations if it were released.

Rationale

Publicly releasing personal information about law enforcement activities or administrative investigations could:

- make it more difficult for Government of Canada institutions to enforce laws or carry out important functions such as protecting national security
- interfere with criminal or other investigations or prosecutions
- reveal techniques used to gather and analyze evidence or intelligence
- hurt relationships with confidential information sources

- make it difficult to make arrests by allowing people or organizations to evade law enforcement officials

Description

As a discretionary exemption, subsection 22(1) states that the head of a government institution may refuse to release personal information requested when:

- the information comes from an investigative body listed in the *Privacy Regulations* and releasing this information could harm law enforcement or conduct of an investigation
- information that, if released, could harm the enforcement of any law of Canada or a province or the conduct of lawful investigations
- information that, if released, could harm the security of penal institutions

Subsection 22(2): Policing services for provinces or municipalities

The Royal Canadian Mounted Police (RCMP) is Canada's national police force. The RCMP often performs policing services for provincial and municipal governments.

Subsection 22(2) of the *Privacy Act* states that a government institution will refuse to release any record that contains personal information that the RCMP obtained or prepared while performing policing services for a province or a municipality.

Rationale

The RCMP gathers personal information while performing policing services for provinces or municipalities.

Subsection 22(2) allows provincial and municipal authorities to get the federal government's cooperation to protect the personal information that the RCMP obtained or prepared in relation to policing services in their jurisdiction.

For example, if the RCMP provided policing services to a municipality in relation to organized crime, the municipality may want to protect that personal information because it relates to future investigations or pending litigation.

Description

Subsection 22(2) states that the head of a government institution will not release any personal information if the federal government has agreed to a request from the province or municipality to protect the personal information that was obtained or prepared by the RCMP while performing policing services for the province or municipality. This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies.

Section 22.1: Information obtained by the Privacy Commissioner

Section 22.1 protects personal information obtained or prepared during investigations by the Privacy Commissioner, such as the details of a complaint that was filed with the Privacy Commissioner.

Rationale

Protecting personal information related to the Privacy Commissioner's investigations helps ensure their ability to perform their duties and powers independently and to facilitate cooperation throughout the investigation.

Description

Subsection 22.1(1) states that the Privacy Commissioner will refuse to release any personal information that was obtained or created by them or on their behalf during an investigation conducted by them or under their authority. This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies.

Subsection 22.1(2) is an exception to 22.1(1) and states that the Privacy Commissioner cannot refuse to release personal information created by them or on their behalf once all investigations and all related proceedings have concluded.

Section 22.2: Public Sector Integrity Commissioner

The Public Sector Integrity Commissioner investigates wrongdoing in the federal public service and helps protect whistleblowers.

To protect people who contact the Public Sector Integrity Commissioner about alleged wrongdoing, the *Privacy Act* requires the Office of the Public Sector Integrity Commissioner to protect personal information in investigation files.

Rationale

Personal information obtained or created by the Office of the Public Sector Integrity Commissioner in an investigation may include sensitive or harmful information, particularly towards a whistleblower.

For example, if a whistleblower contacted the Public Sector Integrity Commissioner with damaging information about practices or negligence by a Government of Canada institution and their personal information became public, the whistleblower may be vulnerable to reprisals.

Description

Section 22.2 requires the Public Sector Integrity Commissioner to refuse to release personal information obtained or created by or for them during an investigation or for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act*. This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies.

Section 22.3: *Public Servants Disclosure Protection Act*

The *Public Servants Disclosure Protection Act* allows federal public servants to report allegations of wrongdoing in their workplace safely and confidentially.

Both the allegations and any potential investigations are often sensitive. The *Privacy Act* requires that heads of government institutions protect any related personal information.

Rationale

The purpose of this exemption is to allow federal public servants to safely report allegations of wrongdoing in the workplace. Section 22.3 protects any personal information created during the entire investigative process.

The ability to report wrongdoings safely not only helps ensure the integrity of the public service, but also protects those who report wrongdoing from reprisals.

Description

Section 22.3 requires the heads of government institutions to refuse to release any personal information requested under the *Privacy Act* that was obtained or created:

- to make a disclosure under the *Public Servants Disclosure Protection Act*
- during an investigation into a release under the *Public Servants Disclosure Protection Act*

This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies.

Section 22.4: Secretariat of National Security and Intelligence Committee of Parliamentarians

The National Security and Intelligence Committee of Parliamentarians (NSICOP) has a mandate to review the legislative, regulatory, policy, administrative and financial framework for Canada's national security and intelligence community. The Secretariat of NSICOP helps it fulfill its mandate.

NSICOP prepares reports for the Prime Minister and Parliament, with sensitive information redacted.

To draft these reports, NSICOP can access any information, with few exceptions, that is under the control of a government institution. This means that the Secretariat may obtain or create highly sensitive records about national security and intelligence.

The *Privacy Act* requires that the Secretariat not release the personal information it has obtained or created.

Rationale

NSICOP members hold the highest level of security clearance and are bound to secrecy by the *Security of Information Act*. This allows them to receive classified briefings and access sensitive materials to review Canada's national security and intelligence organizations.

The Secretariat supports NSICOP in performing their reviews. This organization is made up of public servants who can also access sensitive materials but, unlike NSICOP, the Secretariat is subject to the *Privacy Act*.

To protect national security and intelligence interests, section 22.4 protects all personal information obtained or created by the Secretariat in support of NSICOP's mandate from being released.

Description

Section 22.4 states that the Secretariat must refuse to release any personal information obtained or created by or for it while assisting the NSICOP in fulfilling its mandate. This is a mandatory exemption, and institutions are legally required to withhold personal information where it applies.

Section 23: Security clearances

The government investigates the reliability and loyalty of its employees and contractors. These investigations are conducted when someone is hired and throughout their employment, usually every five to 10 years. The type of work an individual does will determine the frequency and depth of the investigations. Following the investigation, the employee or contractor may be given a security clearance.

Government institutions may collect personal information from the investigative bodies listed in Schedule IV of the *Privacy Regulations* as part of the security clearance process. Information is usually not released when it could reveal the identity of whoever supplied the information. When someone gives an opinion or a statement about someone else, that opinion or statement is considered the personal information of both parties.

This exemption can be applied to security clearances that are required by the Government of Canada or for the government or institution of a province or foreign state.

Rationale

When an investigative body provides a government institution with information on an individual, the expectation is that the source of this information will not be released. The information is shared only for the purpose of determining whether a security clearance should be granted.

Information collected by the government from investigative bodies may contain sensitive personal information about an individual who provided investigative bodies with information about the person undergoing the security clearance. Releasing this personal information and potentially revealing its source could make getting similar information in future, from

the same source or elsewhere, more difficult. Other non-personal information obtained during the security clearance process cannot be protected under this provision.

Description

As a discretionary exemption, section 23 states that the head of a government institution may refuse to release any personal information whose release could reveal the source of information that was obtained or prepared by an investigative body specified in Schedule IV of the *Privacy Regulations*.

That information must have been used to determine whether to grant a security clearance. It should be exempted if the release of the information could reveal the identity of the individual who provided the information.

Section 24: Individuals sentenced to an offence

Correctional Service Canada and the Parole Board of Canada collect personal information about individuals who are sentenced for a federal offence.

The personal information could include the following:

- information about an individual while they are serving their sentence in a government facility
- information that an inmate has provided to the staff of an institution about another inmate
- information about an inmate provided from outside sources
- information about an individual’s compliance with the conditions of their parole or mandatory supervision program, either supplied by the

individual or someone else

Personal information may be exempted from a request while an individual is under sentence. This exemption can continue to apply after their sentence is completed.

Rationale

Providing this type of personal information to a requester may reveal information that was given in confidence. It may also lead the requester to do something that breaches the conditions of their sentence or parole.

For example, information may have been provided to the government that would lead to parole being revoked for an individual. A victim may report that an offender contacted them when no contact is a condition of their release. If confidentiality was promised, this information would not be released.

Description

As a discretionary exemption, section 24 states that the head of a government institution may refuse to release personal information that was collected or obtained by Correctional Service Canada or the Parole Board of Canada while the individual was under sentence for an offence if releasing the personal information could:

- lead to a serious disruption of the individual's institutional, parole or statutory release program
- reveal information about another individual when that individual supplied the information under a promise of confidentiality

Section 25: Safety of individuals

Sometimes, the Government of Canada has or learns of personal information that could put individuals in danger if that information were released.

When the personal information being requested could put one or more individuals in danger, the *Privacy Act* allows the government to protect that personal information from being released.

Rationale

This exemption protects individuals against physical or psychological harm. It does not protect an individual's economic security. The risk to the individual must be serious.

The risk is based on many factors, including past threats made against an individual and the behaviour of the potential offender.

Description

As a discretionary exemption, section 25 states that the head of government institutions may refuse to release any personal information requested if they have reasonable grounds to believe that its release could threaten the safety of an individual.

Section 26: Personal information about another individual

Any information that is recorded about an identifiable individual is considered "personal information." It must be appropriately safeguarded, used and managed in accordance with the *Privacy Act*.

Rationale

Although a requester has a right of access to their own personal information, that right does not extend to information about another individual. This exemption protects an individual's personal information from being released to someone else.

Description

Section 26 protects personal information about another individual held by government institutions from being released.

As a discretionary exemption, this exemption may be applied where personal information about another individual is found in documents that include information about the requester. However, there are three situations where someone else's personal information could be released:

1. where consent is obtained from the other individual
2. where the information is publicly available
3. where the release is allowed under section 8 of the *Privacy Act*, which specifies when personal information can be disclosed without consent

Section 27: Solicitors, advocates and notaries

Government institutions administer and adhere to laws as part of their regular business.

Institutions must act lawfully, and sometimes their decisions or actions can be challenged before the courts. As a result, government institutions frequently employ legal professionals to advise and support them.

Legal opinions, routine communications and litigation files can contain personal information when individuals are involved. The *Privacy Act* allows the government to protect some of this personal information from disclosure when it is subject to solicitor–client privilege.

The solicitor–client privilege exemption refers to two types of privilege: solicitor–client privilege and litigation privilege.

- Solicitor–client privilege, also known as legal advice privilege, applies to all communications between a lawyer and their client relating to seeking or giving legal advice or assistance.
- Litigation privilege applies to records created for ongoing or anticipated litigation.

Rationale

Solicitor–client privilege is necessary to administer justice and maintain the public's confidence in the legal system. It allows clients and their legal professionals to have candid discussions. Clients need to be assured that communications between them and their legal representatives are strictly confidential. Like litigation privilege, this privilege never expires.

Litigation privilege allows litigators to prepare their cases in private without interference by the other party before they make their case in court.

Section 27 ensures that government institutions receive protections for communications with their legal professionals, similar to the private sector.

However, it does not apply where solicitor–client privilege has been waived.

Description

As a discretionary exemption, section 27 states that the head of a government institution may refuse to release personal information subject to solicitor–client privilege.

Section 27.1: Protected information – patents and trademarks

Patents protect inventions, processes and scientific creations from being copied. Likewise, trademarks protect brands, logos and slogans from being copied.

Patent agents and trademark agents are licensed professionals who help clients secure legal protections for their intellectual property by submitting patent or trademark applications.

Section 27.1 of the *Privacy Act* protects privileged communications between clients and their patent or trademark agent.

Rationale

Conversations between patent agents or trademarks agents and their clients may involve sensitive information regarding intellectual property and are privileged in the same way as solicitor–client privilege.

If sensitive information regarding intellectual property was made public, a competitor may use that information to their advantage.

Description

As a discretionary exemption, section 27.1 states that the head of an institution may refuse to release personal information subject to privileges set out in section 16.1 of the *Patent Act* or section 51.13 of the *Trademarks*

Act.

Section 28: Medical records

Sensitive medical or mental health information about an individual may be collected by a government institution, either directly from the individual or indirectly from a medical professional.

Rationale

Government institutions may hold sensitive physical or mental health information about individuals. Although it may be collected, it may not be in the best interests of an individual to be given access to parts of their medical records, especially through a personal information request. Other avenues might be more appropriate.

The decision on what is in the best interest of an individual will be made by the head of a government institution. It is possible for the head to allow a qualified medical professional, such as a psychologist, to review the information so as to provide an opinion on whether to release the information.

The government institution may also require that the requester examine this information in person and in the presence of a medical professional so that the medical professional may explain or clarify the information to the requester.

Description

As a discretionary exemption, section 28 states that the head of an institution may refuse to release any personal information that relates to the physical or mental health of that individual if it would be contrary to the best interests of the individual to view the information.

Sections 13 and 14 of the *Privacy Regulations* outline how medical practitioners or psychologists may help decide what should be released to the requester and how they can help explain and clarify what is released.

Subsection 69(1): Library and museum material

Federal museums and libraries preserve certain information to exhibit or for the public's use. They also accept donations of materials by members of the public, private organizations or representatives acting on their behalf.

The *Privacy Act* does not provide a right of access to materials held in museums or libraries.

Rationale

Museums and libraries preserve material for public reference and exhibition purposes. This includes material donated by private citizens or organizations. This material is protected to prevent the public from accessing the material held by museums or libraries via the *Privacy Act* instead of paying for the services of the museum or library or another third party providing search services.

Description

Subsection 69(1) states that the Act does not apply and grants no right of access to the following categories of information:

- library or museum material preserved solely for public reference or exhibition purposes
- material placed by or on behalf of persons or organizations other than government institutions in the following:

- Library and Archives of Canada
- National Gallery of Canada
- Canadian Museum of History
- Canadian Museum of Nature
- Canada Science and Technology Museum
- Canadian Museum for Human Rights
- Canadian Museum of Immigration at Pier 21

Section 69.1: Canadian Broadcasting Corporation

The Canadian Broadcasting Corporation (CBC) is a Canadian Crown corporation and Canada's national public broadcaster.

It collects and uses personal information for its administrative activities, such as expenditures and staffing, and about their journalistic, creative and programming activities. Examples of these activities include planned stories, the names of key sources and anticipated programming.

The CBC operates at arm's length from the Government of Canada but is still subject to the *Privacy Act.* The *Access to Information Act* excludes information that relates to the CBC's journalistic or creative activities, other than general administration.

Rationale

Freedom of the press is in the *Canadian Charter of Rights and Freedoms*. A free press is important because it means that broadcasters can publish stories without political or public scrutiny or interference.

Since they provide programming other than journalism, broadcasters operate in a competitive environment where each broadcaster wants to attract the most viewers. Releasing planned creative and programming activities could harm a broadcaster's ability to make money from those activities.

Section 69.1 recognizes the unique position of the CBC. Given that it receives government funding, its management functions and administration should be open to public scrutiny as with any other government institution subject to the *Privacy Act*. However, the CBC's specific mandate requires that the same protections extended to private broadcasters apply for CBC's journalistic sources so that it can maintain its creative and programming independence.

Description

Section 69.1 is an exclusion that states that the *Privacy Act* does not apply to any information that is under the control of the CBC that relates to its journalistic, creative or programming activities (for example, show or news anchor selection rationale) other than information that relates to its general administration (for example, personnel files and pay administration files).

Subsection 70(1): Confidences of the King's Privy Council for Canada

The Government of Canada is based on a parliamentary system that includes a Cabinet. The Cabinet is a body of advisors and is a committee of the King's Privy Council for Canada.

Members of the Cabinet are ministers of the Crown who are responsible for government policy. To set policies and priorities for the country, the Cabinet meets regularly to discuss and make decisions on a variety of issues.

The federal public service provides confidential advice to ministers to support their participation in Cabinet. As a result, institutions hold information about Cabinet meetings and discussions. The *Privacy Act* excludes these records, as they are confidences of the King's Privy Council.

Rationale

Releasing Cabinet discussions would harm the Cabinet's ability to discuss issues freely and make informed decisions. The decision-making process and its supporting records are traditionally protected, which enables ministers to have open discussions. Although rare, personal information may be within these types of records but may not be accessible to the individual if the records remain a Cabinet confidence.

Description

Subsection 70(1) states that the *Privacy Act* does not apply to confidences of the King's Privy Council for Canada, including:

- memoranda to present proposals or recommendations to council
- discussion papers to present background explanations, analyses of problems or policy options to council for decision-making
- agendas of council or records of council deliberations or decisions
- records used for or reflecting communications or discussions between ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy

- records to brief ministers of the Crown about matters that are before, or are proposed to be brought before, council or that are the subject of communications or discussions referred to in paragraph 70(1)(d)
- draft legislation

Subsection 70(2) specifies that for the purposes of subsection 70(1), the word “council” means the King’s Privy Council for Canada, committees of the King’s Privy Council for Canada, Cabinet and committees of Cabinet.

Subsection 70(3) specifies that this exclusion has two exceptions:

1. confidences of the King’s Privy Council for Canada that are more than 20 years old
2. discussion papers (see paragraph 70(1)(b)):
    i. if the decisions related to the discussion papers have been made public
    ii. where the decisions have not been made public, if four years have passed since the decisions were made

Section 70.1: Certificate under the *Canada Evidence Act*

Certain Government of Canada institutions conduct criminal and civil prosecutions on behalf of the government. These legal proceedings may involve sensitive information that was obtained in confidence from foreign entities or that relates to national defence or national security.

In national security prosecutions, records about the case may contain information on terrorism offences, war crimes, human smuggling, information that is classified or information obtained from foreign law enforcement partners.

The *Canada Evidence Act* authorizes the Attorney General of Canada to issue a certificate to prevent sensitive information from being released.

The *Privacy* Act excludes information that the Attorney General of Canada has issued a certificate about.

Rationale

For the Attorney General of Canada to issue a certificate, there must be a risk to international relations, national defence or national security. Therefore, that information should be excluded from the *Privacy Act*.

This section ensures that the *Privacy Act* is aligned with the *Canada Evidence Act*. This means that information protected under the *Canada Evidence Act* cannot be released under the *Privacy Act*.

If the Attorney General of Canada issues a certificate after a complaint is filed with the Privacy Commissioner, the complaint is discontinued. The information cannot be released and must be returned to the institution by the Privacy Commissioner.

Description

Subsection 70.1(1) of the *Privacy Act* states that when the Attorney General of Canada issues a certificate under section 38.13 of the *Canada Evidence Act* that prohibits a person's personal information from being released before that person files a complaint under the *Privacy Act* about access to that information, the *Privacy Act* does not apply to that personal information.

Subsection 70.1(2) states that when the Attorney General of Canada issues a certificate under section 38.13 of the *Canada Evidence Act* that prohibits a person's personal information from being released after that person files a complaint under the *Privacy Act* about access to that information:

- all proceedings under the *Privacy Act* about the complaint, including an investigation, appeal or judicial review, are discontinued
- the Privacy Commissioner shall not release the information and shall take all necessary precautions to prevent its release
- the Privacy Commissioner shall, within 10 days after the certificate is published in the *Canada Gazette*, return the information to the head of the government institution that controls the information

Subsection 70.1(3) states that the Privacy Commissioner and every person acting on their behalf or under their direction in the course of their duties must not release information certified under section 38.3 of the *Canada Evidence Act*.

Subsection 70.1(4) limits the power of delegation. Up to a maximum of four officers or employees specially designated within the Office of the Privacy Commissioner may investigate a complaint for information that was subject to a certificate under section 38.13 of the *Canada Evidence Act*.

Date modified:
2023-09-29