Public Inquiry Into Foreign Interference in Federal Electoral Processes and Democratic Institutions | Enquête publique sur l'ingérence étrangère dans les processus électoraux et les institutions démocratiques fédéraux

Overview Report:

Introduction to Intelligence Concepts

Prepared by: Research Council & Commission Counsel

Summary of Report

This report provides a general overview of the meaning of the term “intelligence.” It distinguishes intelligence from “information” and “evidence,” and provides a summary of different forms of intelligence.

The report then discusses the issues that arise when intelligence is disclosed to law enforcement agencies, or is used as part of criminal investigations, or to support administrative decisions that may result in legal proceedings.

Finally, a number of statutory rules meant to address the problems of intelligence being used in legal proceedings are reviewed.

Note to Reader

Pursuant to Rules 42-44 of the Commission’s *Rules of Practice and Procedure*, the following Overview Report contains a summary of background facts and documents relating to the Commission’s mandate.

Overview Reports allow facts to be placed in evidence without requiring the facts and related documents to be presented orally by a witness during the public hearings. Overview Reports may be used to assist in identifying issues relevant to the Commission, make findings of fact and enable recommendations to be made by the Commission.

Parties have been provided an opportunity to comment on the accuracy of this Overview Report. Commission Counsel and the Parties may call evidence from witnesses at the Inquiry that casts doubt on the accuracy of the on the content of the documents underlying this Report. The Parties may also make submissions regarding what, if any, weight should be given to this Report and the cited documents.

Contents

1. Defining Intelligence

1.1 The Purpose of Intelligence

[1] While there is no universally accepted definition of **intelligence**, it is widely understood to describe "information that meets the stated or understood needs of policy makers and has been collected, processed and narrowed to meet those needs."[1] Those needs are typically related to matters of international relations, national defence and national security. These interests may overlap.

[2] In Canada, **foreign intelligence** is defined as information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.[2]

[3] **Defence intelligence** includes all intelligence from the tactical to the strategic level in support of military operations and planning.[3]

[4] **Security intelligence** includes information related to threats to Canadian security stemming from espionage and sabotage, foreign influence, terrorism, violent extremism, and subversion.[4] This is separate from **criminal intelligence** which may also support investigations into these threats to the extent that they are also criminal offences in Canada.

---

[1] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Sage, 2017), **COM0000402**, p. 2.

[2] *Communications Security Establishment Act*, SC 2019, c 13, s 76, s 2, **COM0000385**. See also *Canadian Security Intelligence Service Act*, RSC 1985, c. C-23, s 16(1) **JKW0000015**.

[3] Department of National Defence, DAOD 8008-0, Defence Intelligence, **COM0000387(EN)/COM0000388(FR)**.

[4] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23, s 12, **JKW0000015**.

1.2 Intelligence vs Information

[5] Intelligence is a subset of information. **Information** is anything that can be known, regardless of how it is discovered, its subject matter or its veracity.[5] It is the "unprocessed data of every description which may be used in the production of intelligence."[6]

[6] In short, intelligence is processed information. And while "all intelligence is information, not all information is intelligence."[7]

1.3 The Intelligence Cycle

[7] Intelligence is not only a subset of information. It is also "the process by which specific types of information important to national security are requested, collected, analyzed and provided to policy/decision makers; the products of that process, the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities."[8]

[8] This process is referred to as the "intelligence cycle." The concept commonly includes the following six phases:[9]

a. **Requirements and Direction**. Policy makers present to the intelligence community informational needs and intelligence requirements that reflect the government's policy priorities. Some of these priorities will be long-standing while others will be responsive to issues of the day. In Canada,

---

[5] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Sage, 2017), **COM0000402**, p. 2.

[6] NATO Glossary of Terms and Definitions / Glossaire OTAN de termes et définitions, AAP-06 (2021), **COM0000404**, at 68, 248.

[7] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Sage, 2017), **COM0000402**, p. 2.

[8] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Sage, 2017), **COM0000402**, p. 10.

[9] See e.g. Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 7th ed. (Sage, 2017), Chapter 4, **COM0000403**; Peter Gill and Mark Phythian, *Understanding the Intelligence Cycle*, (Routledge, 2014), Chapter 2, **COM0000405**; CSIS Public Report 2019, **COM0000054**, p. 11.

this occurs every two years through the approval of the intelligence priorities set out in the Intelligence Priorities Memorandum to Cabinet, and the subsequent Ministerial Directives issued to particular intelligence agencies.[10]

b. **Planning.** Intelligence agencies determine how to meet the government's intelligence priorities, including collection plans, the assignment of resources, the need to cooperate with partner agencies, etc.

c. **Collection/Processing/Exploitation.** Intelligence agencies collect information responsive to government priorities using a variety of methods and sources. The type and source of information collected is dependent on the nature of the issue, legal authorities, and the availability of sources. Information collected via technical means may need to be converted, translated or synthesized before it can be used by analysts.

d. **Analysis/Production.** Intelligence analysts examine and evaluate the collected and processed information, add needed context and integrate it into intelligence products. Those products will include an assessment of the subject of the collection (e.g. event, capability, asset, military unit, etc.), and corresponding policy implications. Analysts may also identify intelligence gaps and requirements for additional collection.

e. **Dissemination.** Finished intelligence products are shared with government leaders, officials and policymakers (often referred to as intelligence consumers) to inform decision making. The type of product shared will vary by issue and consumer.

f. **Feedback.** Policymakers evaluate and provide feedback on whether their requirements are being met and if adjustments or improvements are

[10] NSICOP, *Special Report on Foreign Interference in Canada's Democratic Processes and Institutions* (Ottawa: June 3, 2021), **COM0000363(EN)/COM0000362(FR)**, at para. 109; Interview Summary: David Vigneault, Michelle Tessier, Cherrie Henderson, **WIT0000041/WIT0000041.FR**, pp. 2-3.

needed. This feedback may also inform subsequent intelligence requirements and direction.

1.4 Types of Intelligence

[9] Intelligence can be divided into different categories, based on the methods of collection. The most common collection disciplines include:

a. **Human-Source Intelligence (HUMINT).** Information collected by human operators from human sources. For example, copies of confidential documents from a human source.

b. **Signals Intelligence (SIGINT).** The interception of signals, whether between people, between machines, or a combination of both. For example, intercepted radio communications between military units.

c. **Geospatial Intelligence (GEOINT).** Imagery and geospatial data produced through an integration of imagery, imagery intelligence (see below) and geographic information. For example, mapping a foreign state's underwater coastline.

d. **Imagery Intelligence (IMINT).** Representations of objects reproduced electronically or by optical means on film, electronic display devices or other media. For example, satellite images of a foreign military installation.

e. **Measurement and Signature Intelligence (MASINT).** Scientific and technical intelligence information used to locate, identify or describe distinctive characteristics of specific targets. For example, the detection and measurement of nuclear radiation.

f. **Open-Source Intelligence (OSINT).** Publicly available information available in any form, including traditional and social media, public records, academic journals, professional resources, commercial databases or websites. For example, corporate business records.

[10] These categories can be further divided into sub-categories. For example, **communications intelligence (COMINT)** - collected by intercepting communications between two or more people - is a sub-category of Signals Intelligence (SIGINT).

[11] Some sub-categories combine multiple categories of intelligence. For example, **Financial Intelligence (FININT)** and **Social Media Intelligence (SOCMINT)** may combine both Human-Source Intelligence (HUMINT) and Open-Source Intelligence (OSINT).

2. Intelligence-to-Evidence Challenge

2.1 Summary of the Intelligence-to-Evidence Challenge

[12] Government or law enforcement officials may wish to act on the basis of intelligence, which may result in some type of legal proceeding. An example is where police wish to rely on intelligence as part of a criminal investigation, which could result in a charge and criminal trial.

[13] When legal proceedings occur, a further concept becomes relevant: evidence. In this context, evidence is another subset of information, consisting of facts presented before a court, tribunal or other similar body.

[14] The law of evidence sets out rules about:

a. What facts are admissible (i.e. what information can be presented in a proceeding).

b. The method by which those facts may be presented (i.e. how information can be admitted in a proceeding).

c. What inferences can be drawn and how facts are tested and proven (i.e. how information can be used in a legal proceeding once it has been admitted for consideration).[11]

[11] Sidney N. Lederman, Michelle Fuerst & Hamish C. Stewart, *The Law of Evidence in Canada*, 6th ed. (Toronto: LexisNexis, 2022), **COM0000399**, p.3.

[15] In Canada, there are a number of challenges that arise when trying to reconcile intelligence and the intelligence cycle with the standards and expectations of evidence for use in legal proceedings.

[16] Intelligence agencies may share intelligence with government departments and agencies (e.g. police, Transport Canada, the Canada Border Services Agency or the Office of the Commissioner of Canada Elections). Those agencies could theoretically act on this intelligence without worrying about legal proceedings that will result from their actions. However, doing so raises at least two issues.

[17] First, the law may require that a piece of intelligence on which government or law enforcement agencies rely on to take some action be disclosed to the person who is the subject of the action (e.g. criminal charges). This may impact intelligence agencies' interests in preserving secrecy or confidentiality, and possibly make them less inclined to share intelligence. If intelligence agencies are to share intelligence with the understanding that it would be used by government or law enforcement in a way that will result in a legal proceeding, they will usually have to be prepared to have that intelligence disclosed publicly.

[18] Second, the manner in which intelligence is collected may not comply with the rules of evidence, and the intelligence may thus be inadmissible in a legal proceeding. Even if intelligence could be disclosed to an individual or the public, this does not automatically mean that it could subsequently be used in a legal proceeding. In some cases, there will be little or no reason to share or rely on intelligence if it cannot be admitted into evidence. For example, intelligence that is not admissible could not be used to establish an accused person's guilt in a criminal trial.

[19] Both of these issues – disclosure and admissibility – can make it difficult for law enforcement agencies to act upon intelligence. Each also represents a distinct practical challenge in effectively using intelligence in legal proceedings. Where intelligence would be central to a legal proceeding, the refusal to disclose or a finding of inadmissibility may result in a proceeding being terminated. This challenge is commonly referred to as

the "intelligence to evidence" problem. This challenge can manifest itself both in criminal and non-criminal proceedings.

2.2 The Intelligence-to-Evidence Challenge in Criminal Proceedings

[20] Sharing intelligence with law enforcement partners raises questions of how police will use and disclose the information provided. This presents challenges for intelligence sharing when law enforcement may wish to take some action based on shared intelligence.

[21] One challenge arises from the fact that intelligence is not generally collected with the intention that it will be used in a criminal trial. When investigating offences, law enforcement agencies collect information with the knowledge that it may be used as evidence in a criminal trial. Police anticipate that such information will need to comply with the rules of evidence. As a result, law enforcement agencies adopt methods of information collection, retention and sharing that are consistent with the rules of evidence.

[22] Intelligence agencies do not necessarily collect, retain and share information using methods that are consistent with the rules of evidence because this is not their usual purpose for collecting information. While information collected by intelligence agencies may include facts relevant in a criminal investigation or trial, intelligence agencies are not tasked with collecting information for criminal investigations. Consequently, the way intelligence is collected, shared and retained may not comply with the evidentiary standards needed to make it admissible as evidence in a court. This can limit the usefulness of intelligence in criminal proceedings: police may be able to act on intelligence but may not be able to later rely on that intelligence in a subsequent criminal proceeding.

[23] A second challenge in using intelligence in criminal proceedings relates to the rules for disclosing information to people charged with crimes. These rules may be in tension with intelligence agencies' need to keep intelligence secret.

[24] In Canada, a person charged with a crime has a constitutional right to "disclosure." Subject to exceptions for privileged information, the Crown (i.e. the prosecution) has a robust legal duty to disclose information to the defence in a criminal proceeding. This is commonly referred to as **"first party" or "*Stinchcombe*" disclosure**.

[25] The police are required to provide to the Crown all information in their possession relating to the investigation against an accused.[12] The Crown is then generally required to disclose that information to the defence unless it is "clearly irrelevant." [13] All such information must be disclosed to an accused person, without the need for a judge to order the Crown to disclose information.

[26] Information that is not clearly irrelevant must be disclosed, even if:

a. the information is not admissible under the rules of evidence,

b. the information is incriminating and unhelpful to the accused person,

c. the information is not credible, or

d. the Crown has no intention of using the information during the prosecution.

[27] Any information that could reasonably be used by the accused in making "full answer and defence" is relevant. This is the only threshold for disclosure.[14]

[28] The rules respecting disclosure mean that any relevant information shared by intelligence agencies with law enforcement related to a criminal investigation will be subject to disclosure if charges are laid. It could also potentially be used as evidence in court proceedings, and therefore be made public.

[29] Only the information that is disclosed to an accused person can be used as evidence to establish their guilt or innocence in a criminal proceeding. Similarly, if the prosecution wished to rely on intelligence to establish an accused person's guilt, they would be

[12] *R v McNeil*, [2009] 1 SCR 66, at para 23.

[13] *R v Stinchcombe*, [1991] 3 SCR 326 at 338.

[14] *R v Dixon*, [1998] 1 SCR 244 at para 21.

required to comply with the rules of evidence. This could include the obligation to produce a witness to testify under oath and be subject to cross-examination by the accused person.

[30] Disclosure of intelligence provided to law enforcement risks revealing intelligence capabilities, methods and the identity of intelligence officers, sources or targets of investigation. This is information that intelligence agencies seek to protect. The risk that intelligence may be disclosed or used in a criminal trial may cause intelligence agencies to hesitate in sharing intelligence with law enforcement.

[31] This problem is made worse due to the nature of the information generally contained in an intelligence file. Intelligence records often contain information that is unverified: some of this information may be speculative, some may be misleading, some may be no more than rumour. An intelligence agency's investigative holdings regarding an intelligence priority connected to an accused may extend far beyond the scope of a criminal investigation. However, to comply with *Stinchcombe,* it is possible that much of the intelligence file, while unrelated to the criminal charge in and of itself, would not be *clearly irrelevant* to an issue at trial, thereby necessitating its disclosure.

[32] Even if an intelligence agency does not share intelligence with law enforcement, it may still be required to disclose intelligence relating to a criminal investigation. As noted above, only the Crown is subject to first party/*Stinchcombe* disclosure obligations. That said, a "third party" agency that has information relevant to a criminal proceeding may also be ordered to produce that information to the defence. However, a different procedure applies to third parties, commonly referred to as the **"*O'Connor*" procedure**.

[33] Under the *O'Connor* procedure, the accused person has the burden of getting a court order requiring production from a third party. For the defence to succeed under *O'Connor*, they must prove that the records sought are "likely relevant." A record is likely relevant when there is a "reasonable possibility that the information is logically probative to an issue at trial or the competence of a witness to testify,"[15] including "the

[15] *R v O'Connor*, [1995] 4 SCR 411 at para 22.

reliability of other evidence in the case."[16] The likely relevance threshold is higher than the first party/*Stinchcombe* standard of "not clearly irrelevant." The *O'Connor* standard is meant to be "significant, but not onerous."[17]

[34] So long as an intelligence agency maintains its status as a third party, information in its possession and control will be protected from disclosure. The exception is if the accused can meet *O'Connor's* higher relevance threshold. However, if an agency's activities are too closely intertwined with the work of the investigating police force, the agency could be considered a first party, necessitating full *Stinchcombe* disclosure.

2.3 The Intelligence-to-Evidence Challenge in Non-Criminal Proceedings

[35] Intelligence-to-evidence problems also exist outside of criminal prosecutions. There are non-criminal proceedings in which the government may wish to rely on intelligence to take action against an individual. In some cases, this may result in legal proceedings before a court or other body that reviews the government's action, which can engage intelligence-to-evidence problems. Examples of this type of situation include:

a. **Security Certificates.** Proceedings under Division 9 of the *Immigration and Refugee Protection Act* to review a decision of the Minister of Public Safety and the Minister of Immigration, Refugees and Citizenship to designate a person as inadmissible to Canada on the grounds of security, violating human or international rights, serious criminality or organized criminality.[18]

b. **Designation of Terrorist Entities.** Applications to judicially review a decision by the Governor-in-Council to designate an entity as having knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.[19]

---

[16] *R v McNeil*, [2009] 1 SCR 66, at para 33.

[17] *R v McNeil*, [2009] 1 SCR 66, at para 24.

[18] *Immigration and Refugee Protection Act*, SC 2001, c 27, division 9, **COM0000396**.

[19] *Criminal Code of Canada*, RSC 1985, c C-46, s 83.05, **COM0000386**.

c. **Deregistration of Charities.** Proceedings under the *Charities Registration (Security Information) Act* to review a certificate signed by the Minister of Public Safety and the Minister of National Revenue to prohibit the registration of or to deregister an entity that is a charity on the basis that has or would make resources available to a terrorist entity.[20]

d. **Inclusion on the "No-Fly List."** Appeals under the *Secure Air Travel Act* by persons challenging their placement on Canada's "no fly list" of individuals who would threaten transportation security or use air travel to commit a terrorism offence.[21]

[36] These types of non-criminal proceedings do not engage the same type of disclosure right that exists in criminal matters. However, in at least some cases, individuals may have a right to some form of disclosure from the government, which could potentially implicate sensitive intelligence. There are at least three potential sources of a right to some form of disclosure:

a. **Common law procedural fairness.** At common law, there is a presumption that subjects of administrative decisions impacting their rights, privileges or interests receive procedural fairness.[22] Procedural fairness may, depending on the circumstances, require the disclosure of information that is sufficient to permit the individuals to know the case against them and to answer it.[23]

b. **Procedural Rules.** Individuals who are impacted by government decision makers are often able to challenge these decisions in court through a process called judicial review. The statutory rules governing judicial review applications often provide for the production of some type of record of the

[20] *Charities Registration (Security Information) Act*, SC 2001, c 41, s 113, s 5, **COM0000384**.

[21] *Secure Air Travel Act*, SC 2015, c 20, s 11, ss 16-17, **COM0000433**.

[22] *Baker v. Canada (Minister of Citizenship and Immigration)*, [1999] 2 SCR 817.

[23] *Charkaoui v. Canada (Citizenship and Immigration)*, [2008] 2 SCR 326, at para. 58.

proceedings before the administrative decision maker and may in some cases include the information on which the decision was made.[24]

c. **Constitutional and Quasi-Constitutional Rights.** A proceeding that impacts an individual's life, liberty and security of the person, even if it is not criminal in nature, may trigger a constitutional right to some form of disclosure under section 7 of the *Charter of Rights and Freedoms*.[25] Also, the *Canadian Bill of Rights* provides the right to a fair hearing in any proceeding under federal law for the determination of a person's rights and obligations, whether or not the proceeding engages life, liberty and security of the person.[26] This may include a right to disclosure in some circumstances.[27]

[37] In the context of public inquiries, the intelligence-to-evidence problem may emerge in circumstances where a Commission intends to make a finding of misconduct against an individual. Section 13 of the *Inquiries Act* states:

> No report shall be made against any person until reasonable notice has been given to the person of the charge of misconduct against him and the person has been allowed full opportunity to be heard in person or by counsel.[28]

[38] In order to provide procedural fairness to individuals receiving a section 13 notice, such notices "should be as detailed as possible."[29]

[39] If a commission had intelligence suggesting an individual may have engaged in misconduct for the purposes of section 13 of the *Inquiries Act*, a form of the intelligence-to-evidence problem could emerge: on the one hand, the commission could only make

---

[24] E.g. *Federal Court Rules*, SOR/98-106, ss 317-319, **COM0000389**; *Endicott v. Ontario (Independent Police Review Office)*, 2014 ONCA 363 at paras 37-47.

[25] *Charkaoui v. Canada (Citizenship and Immigration)*, [2008] 2 SCR 326.

[26] *Canadian Bill of Rights*, SC 1960, c 44, s 2(e), **COM0000383**.

[27] *Hassouna v. Canada (Citizenship and Immigration)*, 2017 FC 473, at paras 80-98.

[28] *Inquires Act*, RSC 1985, c I-11, s 13, **COM0000397**.

[29] *Canada (Attorney General) v. Canada (Commission of Inquiry on the Blood System)*, [1997] 3 SCR 440, at para 56.

a finding of misconduct if it first provided the individual in question with a section 13 notice. On the other hand, the act of providing a section 13 notice could disclose potentially sensitive intelligence to the person in question. Consequently, a Commission may choose not to, or may have to refrain from making a finding of misconduct in order to not disclose intelligence.

3 Statutory Responses to the Intelligence-to-Evidence Challenge

[40] Parliament has enacted a number of statutory provisions that attempt to respond to the issues that may arise in the attempted use of intelligence as evidence in legal proceedings. This is true both in respect to the problems of admissibility and of disclosure of evidence.

3.1 Statutory Responses to Admissibility Issues

[41] In criminal matters, the issue about whether intelligence meets the admissibility requirements of the law of evidence is a significant one. However, in non-criminal matters, this issue is less of a barrier because the rules of evidence may not apply as strictly. In some types of situations, admissibility questions do not arise in the first place.

[42] For example, in judicial review proceedings, a court reviews the reasonableness of a decision made by a government official. The government official is not necessarily required to comply with the laws of evidence in reaching their decision and can consider a wide range of information, potentially including intelligence products. A reviewing court may consider all the information that was before the decision maker in assessing whether their decision is reasonable. The evidence is admissible before the reviewing court because it was considered by the government official.

[43] In other cases, however, the traditional rules of evidence would normally apply. In these cases, Parliament has enacted statutory rules that remove traditional requirements of the law of evidence. For example, in security certificate proceedings under the *Immigration and Refugee Protection Act*, the *Act* provides that "the judge may receive

into evidence anything that, in the judge's opinion, is reliable and appropriate, even if it is inadmissible in a court of law, and may base a decision on that evidence".[30]

[44] Similar provisions have existed under other federal statutes that involve proceedings that may involve the consideration of intelligence.[31] In 2024 these other statutory rules were standardized under a single set of rules set out in the *Canada Evidence Act*. This regime is discussed in more detail below.

3.2 Statutory Responses to Disclosure Issues

Section 38 of the Canada Evidence Act

[45] With respect to statutory rules designed to respond to the problem of disclosure, the most generally applicable rules are found in section 38 of the *Canada Evidence Act* ("***CEA***").[32] This regime is discussed in the Foreign Interference Commission's *Initial Report*.[33]

[46] In short, the Crown may seek a judicial order with respect to the material that may otherwise need to be produced, on the basis of national security, national defence or international relations interests.

[47] Section 38 may be invoked by any person who, in connection with a legal proceeding, learns that they may be required to disclose sensitive or potentially injurious information, by giving written notice to the Attorney General of Canada ("**AGC**"). Notice is intended to give the AGC the opportunity to review the material to assess whether its release

---

[30] *Immigration and Refugee Protection Act*, SC 2001, c 27, s 83(1)(h), **COM0000396**.

[31] *Charities Registration (Security Information) Act*, SC 2001, c 41, s 113, s 6(j), **COM0000384**; *Secure Air Travel Act*, SC 2015, c 20, s 11, s 16(6)(e), **COM0000433**; *Prevention of Terrorist Travel Act*, 2015, c 36, s 42, s 4(4)(e), **COM0000406**.

[32] *Canada Evidence Act*, R.S.C. 1985, c. C-5. There are some other laws of general application that could also apply to disclosure issues arising from sensitive information. However, due to the central role of section 38 when dealing with intelligence, these other provisions are likely to perform a less significant role.

[33] The Hon. Marie-Josée Hogue, *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions: Initial Report* (Ottawa: Foreign Interference Commission, 2024) at 67-68.

would be injurious to international relations, national defence or national security and, where feasible, enter into a disclosure agreement with the parties. If no agreement can be reached and the AGC has not authorized the disclosure of the information, an application is made to the Federal Court and a specially designated judge will be assigned to adjudicate the matter.

[48] The result of a section 38 proceeding may include the disclosure of some or all the information at issue, the complete withholding of the information, the disclosure of redacted documents or summaries of information, or of written admissions of fact relating to the information.

[49] Section 38 proceedings can result in delays in the underlying proceeding in which the information would otherwise need to be produced. These delays can present challenges to the proper conduct of the underlying proceeding.

[50] Delays caused by section 38 proceedings can present particular challenges when initiated in the context of a criminal prosecution. Delays caused by section 38 proceedings could, depending on the particular circumstances of a case, result in concerns about an accused person's right to trial within a reasonable time under the *Charter of Rights and Freedoms*.[34] A violation of the right to trial within a reasonable time can result in a stay of the criminal proceedings, meaning that a trial will never occur.[35]

[51] Delays caused by section 38 proceedings are less likely to result in a stay of a non-criminal matter, as the right to a trial within a reasonable time only applies to persons charged with an offence. However, it is possible in exceptional circumstances for procedural delays to result in a stay of proceedings in a non-criminal matter.[36]

[52] Non-disclosure of evidence pursuant to section 38 can also have two consequences for criminal proceedings. First, it may limit the evidence that the prosecution can rely on to

[34] *Canadian Charter of Rights and Freedoms*, s 11(b).

[35] For a discussion of the interplay between s. 38 proceedings and s. 11(b) of the *Charter*, see *R v Huang*, 2021 ONSC 8372.

[36] *Blencoe v. British Columbia (Human Rights Commission)*, [2000] 2 SCR 307.

prove its case, since evidence that is not disclosed to an accused person cannot be relied upon as evidence to convict them at trial. This could lead a prosecutor to withdraw some or all charges.

[53] Secondly, non-disclosure of information to an accused person may impact their constitutional right to make full answer and defence. If a trial judge concludes that non-disclosure of information would impact the fairness of the trial, they may issue a remedy up to and including a stay of the prosecution. This remedy is available under both the *Charter of Rights and Freedoms*[37] and pursuant to the section 38 statutory scheme itself.[38]

Other provisions dealing with sensitive information

[54] While section 38 applies broadly to all proceedings, Canadian law also has special provisions dealing with sensitive information, including intelligence, in particular types of proceedings. These provisions attempt to address fairness issues engaged by the intelligence-to-evidence problem through two tools: providing individuals with summaries of information that is too sensitive to disclose; and the use of security-cleared lawyers who have access to sensitive information and who advance the interests of the impacted individual.

[55] For example, under the "security certificate" regime in the *Immigration and Refugee Protection Act*, Ministers may rely on classified intelligence when determining an individual is inadmissible to Canada on security-related grounds.[39] These decisions are automatically reviewed in the Federal Court.

[56] In these proceedings, while the Court can access all the information relied on by the Ministers, the subject of the security certificate cannot. They are prohibited from accessing any information the disclosure of which could be injurious to national security

---

[37] *Canadian Charter of Rights and Freedoms*, ss. 7, 11(d).

[38] *Canada Evidence Act*, RSC 1985, c C-5, s 38.14; *R. v. Ahmad*, [2011] 1 SCR 110, at paras 34-35.

[39] *Immigration and Refugee Protection Act*, SC 2001, c 27, division 9, **COM0000396**.

or could endanger the life of any person.[40] Instead, the individual receives "a summary of information and other evidence that enables them to be reasonably informed of the case made by the Minister in the proceeding".[41]

[57] The Court must also appoint a "special advocate," who is a security cleared lawyer whose job is to protect the interests of the subject of the security certificate in proceedings where the Court is hearing evidence in the absence of the public and the subject of the certificate. The special advocate is not counsel to the individual, but acts in their interest as an alternative to the individual and their own lawyer having access to the sensitive information being relied on.[42]

[58] The special advocate regime has been found to be constitutional. However, the Supreme Court of Canada says there is "an incompressible minimum amount of disclosure that the named person must receive" even with the protections of a special advocate. This minimum core of required disclosure is "sufficient disclosure to know and meet the case against" the person.[43] What this means in practice varies from case to case.

Bill C-70 general framework for judicial review proceedings

[59] A new legislative framework for addressing some intelligence-to-evidence issues was implemented through Bill C-70, which received Royal Assent on 20 June 2024 and came into force on 19 August 2024.[44] Amendments to the *Canada Evidence Act* establish a general framework for federal judicial review proceedings in which a participant anticipates disclosing information that is sensitive on the basis of national security, national defence or international relations interests.[45]

---

[40] *Immigration and Refugee Protection Act*, SC 2001, c 27, s 83(1)(c), **COM0000396**.

[41] *Immigration and Refugee Protection Act*, SC 2001, c 27, s 83(1)(e), **COM0000396**.

[42] *Immigration and Refugee Protection Act*, SC 2001, c 27, ss 83(1)(b), 85.1, **COM0000396**.

[43] *Canada (Citizenship and Immigration) v. Harkat*, [2014] 2 SCR 33, at para 54.

[44] *An Act Respecting Countering Foreign Interference*, SC 2024, c 16, **COM0000381**.

[45] *An Act Respecting Countering Foreign Interference*, SC 2024, c 16, s 84 **COM0000381**.

[60] The scheme incorporates elements of both the section 38 framework and the special advocate regime. When a person believes that information that may be injurious to national security, national defence or international relations may be disclosed in a judicial review of a federal decision, they must provide notice to the AGC. Similar to the section 38 regime, this notice triggers a process whereby the government may either negotiate an agreement to release certain information or litigate the issue of disclosure.[46]

[61] The court that is judicially reviewing the federal decision may still rely on information that is not disclosed to the individual pursuant to these rules. However, they may appoint a special counsel to protect the interests of the individual in question.[47]

[46] *Canada Evidence Act*, RSC 1985, c C-5, ss 38.2 – 38.26, as amended by the *Countering Foreign Interference Act*, SC 2024, c 16, s 84, **COM0000381**. Note, a consolidated version of the *CEA* has not yet been published by the Department of Justice.

[47] *Canada Evidence Act*, RSC 1985, c C-5, ss 38.33 – 38.35, as amended by the *Countering Foreign Interference Act*, SC 2024, c 16, s 84, **COM0000381**. Note, a consolidated version of the *CEA* has not yet been published by the Department of Justice.