Addressing foreign interference

This document outlines a range of issues and approaches for consultation, and does not constitute the Government of Canada's final position.

Whether to Amend the *Security of Information Act* and Modernize certain *Criminal Code* offences, and to Introduce a review mechanism in the *Canada Evidence Act* to manage sensitive information

Context

As an advanced economy and open democracy, Canada is often targeted by foreign states, or those acting on their behalf, seeking to advance their own strategic objectives. While foreign states usually advance their interests in legitimate and transparent ways, some also act in ways that threaten or intimidate people in Canada, their families elsewhere or are covert and deceptive, and harmful to Canada's national interests.

Often described as foreign interference, these deceptive, coercive and threatening activities can target all levels of government, the private sector, academia, diverse communities and the general public.

We know that in Canada, threat actors seek, among other things, to:

- Attack or undermine the integrity of democratic institutions, and covertly influence the outcomes of electoral processes, including the nomination of candidates.
- Cultivate influential people to sway government decision-making and policies to advance their interests, and discredit those who threaten their interests,
- Intimidate or harass individuals, who speak out against repression in foreign states, in attempts to stamp out dissent and limit democratic rights and freedoms on Canadian soil, as part of a campaign of transnational repression,

- Intimidate the families of these individuals who reside in those foreign states,
- Steal Canadian-made knowledge, expertise, know-how, and innovation to support their own military or economic objectives,
- Undermine the legitimacy of Canada's representatives abroad, or the goals of the Canadian government's international activities, and
- Insert themselves into Canada's supply chains and critical infrastructure.

While foreign interference activities are not new, they have increased in volume and complexity in recent years. This is why, more than ever, Canada must be equipped with the necessary tools to take proactive and decisive action against the threats posed by foreign interference.

Existing Measures

The Government currently uses various measures to counter foreign interference, including investigating and laying criminal charges in accordance with Canadian laws. These laws include Canada's *Security of Information Act* (SOIA), which criminalizes information-related conduct that may be harmful to Canada, such as spying, economic espionage and foreign-influenced threats or violence. There are *Criminal Code* offences that address different types of conduct in connection with foreign interference, such as sabotage, intimidation, computer hacking and bribery, amongst others. In addition, there are offences and other provisions in the *Canada Elections Act*, which address foreign involvement in our federal electoral processes. For example, it is an offence for a foreign individual or entity to unduly influence an elector's vote. It is also an offence for third parties in an election to use foreign funds for their activities.

In recent years, however, many experts have called on Canada to modernize its laws to address new and evolving foreign interference threats, such as those emanating from emboldened and assertive foreign states, and the growth of community and online media and social media avenues for threats and other forms of interference, and to ensure consistency with allied countries. The SOIA, for example, has not had a substantial revision since 2001 and may benefit from updates that would better respond to modern threats. Australia and the UK have recently taken steps to enhance their ability to identify and counter foreign interference.

Key concerns with the existing legal framework include uncertainty as to whether conduct linked to foreign interference would always be adequately captured under existing laws, or would provide police and prosecutors with enforceable foreign interference offences that are consistent with the *Canadian Charter of Rights and Freedoms* (the Charter), including freedom of expression which includes freedom of the press.

Section 20 of the SOIA, for example, addresses foreign interference, but only in a limited way. The offence is limited to circumstances where someone uses threats or violence to advance the interests of a foreign entity, and the burden is on the prosecution to show that the purpose was to increase the capacity of a foreign entity to harm Canadian interests, or where the threats or violence are reasonably likely to harm Canadian interests. It does not cover, for example, other types of non-violent foreign interference, including interference with democratic processes. Some other acts may be an offence under the *Criminal Code* or other statutes, but existing criminal offences that are committed for the benefit of foreign states may not fully reflect the serious impact of the foreign interference.

The Government is assessing whether it is desirable and appropriate to amend the criminal law to address these concerns. This consultation paper describes how existing provisions could be modernized, such as the dated sabotage offence in the *Criminal Code*.

Similar to recent reforms in the UK and Australia, it also proposes to create new offences that respond to the modern threat landscape. The amendments being considered could provide more certainty as to what activities would be criminalized as foreign interference, and provide penalties that reflect the seriousness of such activities. In addition, the Government is considering whether there are ways to enhance deterrence by increasing the risks to foreign entities considering such activities in Canada.

Furthermore, this consultation paper seeks input on measures that could be taken to provide an overall legislative scheme in the *Canada Evidence Act* and the *Criminal Code* for the protection and use of national security information in judicial reviews and statutory appeals of governmental decision-making. Finally, it will seek views on potential reforms regarding how national security information is used and protected.

Respecting Individual Rights and Freedoms

The Charter sets out the fundamental rights and freedoms that we, as a country, believe are necessary in a free and democratic society. The Charter applies to all levels of government and protects the following: fundamental freedoms, including freedom of expression and democratic rights; the right to live and seek employment anywhere in Canada; legal and equality rights; the official languages of Canada and minority language education rights; Canada's multicultural heritage; and the rights of Indigenous peoples.

Subject to a few exceptions, including the right to vote and the right to enter, remain in and leave Canada, any person in Canada – whether a Canadian citizen, permanent resident or newcomer – benefits from the rights and freedoms contained in the Charter.

The SOIA and *Criminal Code* can affect rights that are protected by the Charter, as well as the public interest, in various ways. In the national security context, legitimate concerns have been raised as to whether government powers to address serious threats to Canada's safety and security unnecessarily impede individual rights and freedoms, such as freedom of expression under section 2(b), the right to life, liberty and security of the person under section 7, and the right to be free from unreasonable search and seizure under section 8 of the Charter.

Any new amendments to Canada's laws that protect against foreign interference will give rise to legitimate worries about the protection of other important values, rights, and interests. With this in mind, it is crucial that any reforms strike an appropriate balance between ensuring an effective criminal justice response to foreign interference and respecting the fundamental rights and freedoms of people in Canada.

These illustrative scenarios might help explain what is meant by foreign interference:

Scenario 1

Ms. M is community organizer in a small Canadian city. Her family and friends have encouraged her to run for elected office. Because Country F disagrees with her views, Country F initiates a disinformation campaign against her, with the help of other people in Canada. The disinformation campaign targets the supporters of Ms. M and aims to create confusion about her campaign with false narratives. Country F interferes with her nomination campaign by sending confusing information to her supporter about when, where, and how to vote for Ms. M.

Scenario 2

Mr. A is a student attending a Canadian university. They organized a series of on-campus protests against Country X, a foreign state that is known to violate the human rights of minorities, based on their religious beliefs and racial ethnicity. Mr. A (as the organizer) and participants begin to receive threatening and harassing emails, social media messages, and phone calls. Mr. A's personal information, and that of other participants, is also posted online, and family members begin to receive threats. Country X has been involved in the coordination of this harassment campaign.

Scenario 3

Ms. C is a permanent resident that emigrated from Country Z. She has lived in Canada for several years, but recently started receiving emails and phone calls from individuals identifying themselves as security officials from Country Z telling her to return home to face prosecution for alleged crimes. She has received visits from unknown individuals at her residence claiming to be officials from Country Z advising her to return home. She has also received recent photographs of herself and her family members in the mail. She suspects that she is being followed, and that spyware might have been installed in her personal electronic devices, as the callers know personal and private information, including where she lives, her family and friends, and where she works. The phone calls are increasingly hostile and threatening; most recently, she has been told that if she does not return home, her family members in Country Z will be arrested and tried for her alleged crimes.

Issue 1: Whether to Create New Foreign Interference Offences

Context

The SOIA already addresses foreign-influenced or terrorist-influenced threats. Section 20 includes an offence of inducing someone, using violence or threats, to do anything to help a foreign entity (including a foreign state) or a terrorist group harm Canadian interests. Harm to Canadian interests is caused when a foreign entity or terrorist group does anything set out in section 3 of the SOIA, which sets out what prejudices the safety or interests of Canada. This includes, for example, conduct that endangers the lives, health or safety of

Canadians, threatens the Government's ability to defend Canadian sovereignty, or interferes with services or systems tied to the economic or financial well-being of Canadians. The offence carries a maximum penalty of imprisonment for life.

Why create new offences?

Some argue that the current offences do not always capture the latest ways that foreign interference is affecting people in Canada. Allies, like Australia, have recently amended and strengthened their foreign interference laws, including by creating many new offences to deal with the modern threat environment, such as improved espionage and sabotage laws, and a law addressing interference with political rights and duties.[1] This year, the UK introduced new foreign interference offences.[2] In 2020, Amnesty International called on Canada to examine legislation in other jurisdictions countering covert foreign interference and consider enacting similar legislation in Canada.

The Government is considering criminal law amendments to the SOIA to address the challenges of foreign interference.

What alternatives are we examining to better address these situations?

The SOIA could add clarity to the criminal law in relation to foreign interference by adding new offences that would ensure that there are no gaps in the law, including:

Commission of an Indictable Offence for a Foreign Entity

- A new offence could provide that it is an offence to commit an indictable offence for the benefit of or at the direction of a foreign entity.
- Similar offences exist in the *Criminal Code* in relation to terrorism and organized crime.

Such an offence would make it clear that it is a very serious matter to commit a criminal offence on behalf of a foreign entity.

---

[1] Australia's law, the *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* is found here: https://www.legislation.gov.au/Details/C2018A00067

[2] The United Kingdom's *National Security Act 2023* is found here: https://www.legislation.gov.uk/ukpga/2023/32/contents/enacted

- For example, it is an indictable offence under the *Criminal Code* to use deceit, falsehood or other fraudulent means to defraud the public or a person of money or property (section 308(1)). Imagine that J poses as a legitimate financial institution and lures an individual to transfer money by email (i.e. phishing), and that J is participating in this fraud to raise funds to in support a foreign state.[3]

Foreign Interference Offence – General

- There could be a new SOIA offence of knowingly (or recklessly) doing anything, or omitting to do any covert or deceptive act for the benefit of a foreign entity, knowing that it would cause harm to Canadian interests. It would apply whether or not the underlying act is a criminal offence.
- The offence would expand the scope of the current *Security of Information Act*, which relates to foreign-influenced threats or violence, to capture persons who engage in these activities. As with the section 20 offence, the harm to be protected against by the offence could be tied to the existing harms set out in section 3 of the SOIA, or to a new harm that could be developed.
- One example could be knowingly facilitating the entry into Canada of agents of a foreign entity who are posing as tourists. Another example could be planting false stories to discredit a critic of a foreign government.
- The offence would not apply to legitimate activities performed for the benefit of a foreign entity that are not covert or deceptive, for example, promoting a foreign country's industry, language, or culture, or diplomatic activities, or transparent lobbying for a foreign country's interests.

Foreign Interference – Intimidation (Harm Specific to the Person) or Inducement

- As noted above, Section 20 of the SOIA already criminalizes foreign-influenced threats or violence, which induce or attempt to induce a person to do anything, or to refrain from doing anything, where there is a threat of personal harm.

[3] All of the examples provided in this consultation paper are for illustrative purposes only. They should not be relied on as definitive statements regarding possible criminal liability given that they are hypothetical, and are presented in advance of any potential amendments to the law. Establishing that all of the elements of a particular foreign interference offence have been established would be a matter determined by a criminal court, following an investigation by law enforcement officials and a prosecution by an independent prosecution service. This information does not constitute legal advice.

- A new offence would make the current section 20 offence more straightforward by removing the requirement that there be proof that it actually helped the foreign state or harmed Canada. Instead, all that would be required is that the threat or violence was done on behalf of, or in association with a foreign state.
- For illustrative purposes, the proposed offence could potentially address scenarios 1, 2 and 3 above.

Foreign Interference – Democratic Process

- The *Canada Elections Act* contains measures to address potential foreign interference threats to federal elections. This includes section 282.4, which makes it an offence for certain persons, including an individual who is not a Canadian citizen or permanent resident, a foreign corporation or entity, a foreign political party, a foreign government or its agent, to, during an election period, unduly influence an elector to vote or refrain from voting, or to vote or refrain from voting for a particular candidate or registered party, at a federal election.
- To complement the *Canada Elections Act*, there could be a new offence to protect the democratic processes and elections at all levels of government. This new offence would apply at all times, including outside of the election period.
- The new offence would cover the situation where a person engages in conduct for the benefit of a foreign entity, where the conduct is covert or involves deception, and where the person intends that the conduct will influence a political or governmental process, or will influence the exercise of a democratic right or duty, in connection with Canada.
- This new offence would improve the protection of Canada's democracy, and could be similar to an offence found in the *Australian National Security Legislation Amendment (Espionage and Foreign Interference) Act, 2018*.
- This offence would address Scenario 1 outlined in the box above. It would be carefully drafted so as not to capture legitimate democratic activity, including the free exchange of ideas and controversial views that may occur in connection with the functioning of Canada's democratic processes. It would not prevent foreign states, through their representatives, from expressing their views, or lobbying for their country's interests, in a transparent way.

- If implemented, the proposed offence could capture the following situation: A community organization representing members with a connection to Country X uses social media to support the exchange of ideas and opinions amongst its members. During a municipal election, it makes a series of posts endorsing policies advanced by a political party and encourages its members to vote for that party. The posts contain disinformation about the issues of relevance to the election. The community organization secretly receives pressure from Country X to post this disinformation that it knows to be untrue on social media upon the threat of losing funding from Country X, which supports community welfare and outreach activities.

What do you think?

1. Should Canada have additional "foreign interference" offences to ensure that we have covered situations like those described in the scenarios? If so, which of the four new offences above do you think would be beneficial?
2. Instead of creating new offences, would it be better to give the judge the ability to increase the penalty when sentencing an individual, if the crime was committed for the benefit of a foreign entity? It may be easier for prosecutors to deal with this issue as an aggravating factor at the sentencing stage, as is done with terrorism offences. This way, if a prosecutor is unable to establish the foreign link, the underlying offence could still be proven. Or should the law do both?
3. What kinds of activities of foreign states are unacceptable in Canada, keeping in mind that Canadian officials are involved in legitimate efforts to advance Canadian interests abroad?
4. The SOIA already defines the term "foreign entity" as five things: a foreign power; a foreign power and one or more terrorist groups; a group or association of foreign powers; a group or association of foreign powers and one or more terrorist groups; or a person acting at the direction of the first four entities. Do we need to expand what we mean by "foreign entity" in relation to these offences?
5. Keeping in mind the protections that already exist in the *Canada Elections Act*, and in provincial elections legislation, what sorts of democratic processes, rights and duties warrant protection from foreign interference under the SOIA?

Issue 2: Whether to amend section 22 of the *Security of Information Act* (SOIA) to increase the maximum penalty and to have it apply to other offences

Context

Section 22 of the SOIA is a preparatory acts offence, meaning that it is an offence to do anything in preparation of the commission of certain other SOIA offences. These include espionage, economic espionage, communication of special operational information to a foreign entity or to a terrorist group, and foreign-influenced threats of violence. This offence provides the ability to investigate and prosecute a person before the person has caused, or actually attempted to cause, harm to Canada, where a real threat to security exists. The offence is intended, for example, to address the issue of "sleeper" agents and others who participate, at the early stages, in carrying out a foreign interference activity. It is punishable by a maximum term of imprisonment of not more than two years.

Section 23 of the SOIA also captures conspiracies and attempts. A person who conspires or attempts to commit an offence, is an accessory after the fact in relation to, or who counsels in relation to an offence under this Act, is liable to the same punishment as if they themselves had committed the offence.

Why amend section 22?

Some have argued that a maximum term of two years imprisonment for preparing to commit one of these offences does not reflect the seriousness of the offence, when compared to similar offences in the *Criminal Code*. Expanding the coverage (to have it apply to more or all of the SOIA offences) is also something that could be considered in order to better address foreign interference threats.

What alternatives are we examining to better address these situations?

The maximum penalty available on conviction for this offence could be increased. There is a criminal law principle that the carrying out of an offence that results in actual harm deserves a higher penalty than preparing to commit that offence. The penalty could be amended so that there would be a maximum penalty of five years for the preparatory offence in connection with an SOIA offence that is punishable by a term of imprisonment of ten years or more.

The preparatory offence in the SOIA resembles in some ways the offence of "participation in the activity of terrorist group" in section 83.18 of the *Criminal Code*. The main difference is that the SOIA offence usually arises in connection with foreign states instead of terrorist groups. The maximum penalty available for section 83.18 is a term of ten years. The preparatory offence under SOIA currently applies to only certain other offences in the Act: ss. 16(1) or (2) (Communicating safeguarded information), 17(1) (Communicating special operational information), 19(1) (Use of trade secret for the benefit of foreign economic entity), and 20(1) (Foreign-influenced or terrorist-influenced threats or violence).
The preparatory offence could also be amended so that it applies to more SOIA offences, including:

- The offence in section 6 of approaching or entering a prohibited place for purposes prejudicial to the safety of the State;
- The offence in section 7 of interfering with a peace officer or a member of the Canadian Forces on guard or patrol duty in the vicinity of a prohibited place; and
- The offence in section 14 for unauthorized communication of special operational information.

Currently, the preparatory offence does not apply to any of these three offences. A person who commits an offence under these provisions is liable to a maximum penalty of 14 years imprisonment, but currently there is no offence for preparing for the commission of these offences.

What do you think?

1. Is a maximum term of imprisonment of five years (as opposed to the existing two years) the appropriate penalty for preparatory acts that fall short of the full act of either espionage, communication of special operational information to a foreign entity or to a terrorist group, and foreign-influenced threats of violence?
2. What is the appropriate maximum penalty for preparatory acts relating to economic espionage (currently 2 years)?
3. Are there other offences in the *Security of Information Act* to which this provision (preparatory acts offence) should apply?

Issue 3: Whether to Modernize Canada's Sabotage Offence

Context

Sabotage can be described as various activities that target infrastructure, electronic networks, systems, property, and other things, carried out with the goal of endangering a country's safety and security interests. For instance, by disrupting supply chains or damaging infrastructure that are vital to everyday life in Canada, a foreign state can harm Canada's political institutions, economy and communities.

The *Criminal Code* contains an offence for sabotage, which criminalizes conduct that jeopardizes the safety, security or defence of Canada, or that of military forces of other states that are lawfully in Canada (section 52). This includes acts or omissions meant to impair the efficiency or impede the working of any vessel, vehicle, aircraft, machinery, apparatus *or other thing*. It also includes conduct that causes property to be lost, damaged or destroyed.

The sabotage offence contains exemptions from criminal liability, such as work stoppages related to labour disputes or safety concerns. A person who goes near a place only to obtain or communicate information is likewise exempted from this offence.

Other *Criminal Code* offences can apply to protect infrastructure from similar damage, such as unauthorized use of computer (section 342.1); possession of a device to obtain unauthorized use of computer (section 342.2); mischief (section 430); and delivering explosive or other lethal device used against a public place, government facility, or a public transportation system or infrastructure facility an (section 431.2).

Why modernize the sabotage offence?

Canada's allies, such as Australia and the United Kingdom, have pursued reforms that focus on clarifying what infrastructure is captured by their sabotage offence, expanding the types of prohibited conduct and adding a foreign interference element. This raises the question of whether Canada should do the same.

Whether providing access to clean water and reliable sources of energy, safe transportation systems or secure information and communication technology, essential infrastructure plays a key role in the delivery and support of daily necessities for Canadians. It follows that acts of foreign interference that disrupt essential infrastructure pose a serious threat to Canada. Such acts could lead to

catastrophic loss of life, negative economic consequences and harm to public confidence.

Modernizing the sabotage offence in Canada's *Criminal Code* would ensure that it is responsive to the evolving threats posed by foreign interference, and support broader efforts to protect Canada's essential infrastructure. It is worth noting that in his Report of the Public Inquiry into the 2022 Public Order Emergency, Commissioner Rouleau recommended that the federal government should initiate discussions with provincial and territorial governments, in consultation with Indigenous governments and affected municipalities, to promptly identify critical trade transportation corridors and infrastructure, and establish protocols to protect them and respond to interference with them.[4]

What alternatives are we examining to better address these situations?

The sabotage offence would still target a person who purposely engages in conduct that jeopardizes the safety and interests of Canada, or that of military forces of other states that are lawfully in Canada. The goal of potential amendments would be to:

- Clarify that the offence applies to public and private infrastructure that is essential to the health, safety, security and economic well-being of Canadians. This could include, for example, systems that enable transportation or communications, provide access to clean water and energy, support the delivery of health and food services, and facilitate Canada's security and defence;
- Build on the existing conduct prohibited by the offence, by broadening the range of acts or omissions threatening essential infrastructure. This could include, for instance, interfering with, abandoning, or limiting access to essential infrastructure in order to cause its loss or make it inoperable, unsafe or unfit for its purpose;
- Add a new element to the offence, or create a separate sabotage offence, requiring that the person carrying out the sabotage work on behalf of foreign entity. This could include a person being funded by and/or acting under the instructions of a foreign entity. It could also capture conduct intended to benefit a foreign entity.

[4] https://publicorderemergencycommission.ca/final-report/

- Add a companion offence to criminalize making, possessing, selling and/or distributing a device to commit the offence of sabotage. One example of such a device would be a "bot", which is an Internet-connected device that is infected with malware.

Striking the right balance between public safety objectives and potential impacts on Charter protected rights and freedoms is essential in considering any amendment to the sabotage offence. The broader the scope of the offence, the greater the potential impact it may have on Charter protected rights and freedoms including on freedom of expression and freedom of peaceful assembly rights.

Charter protections

- The sabotage offence currently contains certain protections to ensure that damage to infrastructure resulting from labour action like work stoppages cannot constitute sabotage. The existing exemptions in the sabotage offence would be maintained, and could be further expanded to include other forms of lawful dissent such as protests. The exemptions included in the terrorism provisions of the *Criminal Code* could be used as a model in this regard.
- As an additional safeguard to protect legitimate forms of dissent and advocacy, consideration could be given to requiring the consent of the Attorney General before proceeding with charging someone with an offence under this provision. There are several Attorney General consent provisions in the *Criminal Code*, and in other statutes, for example, consent of the Attorney General is required to proceed with a charge for hate propaganda or public incitement of hatred.[5] With such a safeguard, the public interest in any prosecution would be assessed at a higher level, by an official who is well placed to assess the public interest, having regard for the potential impacts on fundamental freedoms.

What do you think?

1. Should the law of sabotage be updated to ensure it covers modern forms of critical infrastructure such as water, sewage, energy, fuel, communication, and food services? Should it be updated to clarify that it covers a broader range of

[5] See for example *Criminal Code* s 7 (certain offences committed outside of Canada by non-Canadians), s. 83.24 (proceedings in respect of terrorism offences), s. 318 (hate propaganda), 319 (public incitement of hatred), the Special Import Measures Act, the Geneva Conventions Act, s. 3(4), among several other offences.

negative impacts on infrastructure? Or, would it be enough to rely on existing offences such as unauthorized use of computer; mischief; use of an explosive or other lethal device against a government or public facility, public transportation or other infrastructure?
2. Would it be beneficial to give the judge the ability to increase the penalty, when sentencing an individual, if the crime was committed for the benefit of a foreign entity?
3. Are the existing exemptions from liability still appropriate? Should other exemptions be considered, like those found in the terrorism provisions of the *Criminal Code*? Should there be a requirement to get the consent of the Attorney General to proceed with the offence?
4. Would it be appropriate to create an offence to capture possession of a device to commit sabotage? Should such an offence require intent to commit sabotage? What kinds of devices would be appropriate to include in such an offence?

Issue 4: Whether to Create a General Secure Administrative Review Proceedings Process under the *Canada Evidence Act*

Context

Section 38 of the *Canada Evidence Act* addresses the disclosure and use in legal proceedings (whether criminal, civil, or administrative) of information that could be injurious to international relations, national defence, or national security (sensitive information).

Currently, the application of these disclosure rules occurs via a separate process, where a designated judge of the Federal Court will examine the sensitive information involved in the underlying and separate legal proceeding and will rule on both the claim of privilege and whether and how to disclose it to the non-governmental party (fully or partly redacted or as a summary or agreed statement of facts, with conditions). This occurs even where the main proceeding is not in the Federal Court.

Sensitive information may be relevant in a range of federal administrative statutory decision-making processes, including in foreign interference matters. Administrative decisions relating to foreign interference could come up in any

number of situations – from federal decisions involving companies, investments, licences to security clearances.

Whether the decision-maker is a government official, tribunal or Minister, these decisions may eventually be subject to judicial review or appeal in Federal Court. This creates a situation where sensitive information may be involved in an open legal proceeding. Where this occurs, the existing law will usually protect this information from disclosure but, generally speaking, does not allow the court to consider any of the protected information when adjudicating the matter before it. A basic principle of adjudicative fairness is that all parties receive the same access to the factual record being considered by the adjudicator (such as a court).

Therefore, when an affected party challenges a government decision that was premised upon sensitive information in the courts, the government faces a difficult choice: protect the information used to make this decision from disclosure, and risk having that decision quashed on judicial review or statutory appeal, or disclose the sensitive information to the Court and the non-Government litigant, and experience the corresponding national security operational impacts associated with that disclosure.

Stand-Alone Regimes

To date, Parliament has enacted several stand-alone closed proceeding authorities which expressly authorize the Federal Court to both protect sensitive information from disclosure and rely upon it while determining the merits of an application for judicial review (or a statutory appeal). These include:

- *Charities Registration (Security Information) Act*, (2001) ss. 6, 11(2) - a process in the Federal Court for reviewing Ministerial decisions regarding the denial or revocation of charitable status for national security grounds.
- *Criminal Code*, (2001) ss. 83.05(6), 83.06 - judicial review in Federal Court of a Ministerial decision on a de-listing application.
- *Prevention of Terrorist Travel Act*, (2015) ss. 4(4), 6(2) - judicial review in Federal Court for the cancellation of a passport on national security grounds.
- *Secure Air Travel Act*, (2015) ss. 16(6), 17 - appeals in the Federal Court of Ministerial directions concerning orders, no fly lists, denied boarding and screening.
- Closed proceedings in the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism* (2001).

- *Criminal Code*, (2023) amendments that create a regime allowing the Minister of Public Safety to issue authorizations to persons and organizations permitting them to undertake humanitarian relief activities in areas controlled by a terrorist group that would otherwise be prohibited under subsection 83.03(2).
- *Bill C-26 (An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts)*.
- *Bill C-34 (An Act to amend the Investment Canada Act)*.

These regimes typically also require the Federal Court to ensure that the affected individual has been reasonably informed of the content of the information before the Court, and gives the Federal Court sufficient flexibility to ensure a fair judicial process. Such stand-alone regimes exist at the judicial stage.

Variations in the stand-alone regimes

One possible drawback of adding new standalone regimes is that there are often variations between the regimes. These variations could lead to errors, confusion, and inconsistent outcomes in the assessment of national security information when decisions are judicially reviewed.

Lack of a generally applicable process and the foreign interference context

Another concern is that for judicial reviews of decisions not covered by the existing stand-alone regimes, there is no ability for a judge to both protect sensitive information from disclosure and rely upon it while determining the merits of an application for judicial review (or a statutory appeal). It is not always possible to predict when national security information will be at issue in an administrative decision. Having a generally applicable scheme would ensure that national security information can be protected from disclosure and relied upon as necessary whenever it arises.

For example, there is currently no closed-proceeding authority that applies to the review of administrative decisions relating to foreign interference. As explained above, in the absence of such a judicial authority, the Government would not have the ability to protect the sensitive information from disclosure while also relying upon it to defend the merits of an administrative decision being challenged in the courts. Where the operational impact of disclosing the sensitive information is significant, this may prevent the Government from putting the most complete

decision-making record possible before the reviewing court, negatively impacting the Government's ability to defend the decision in question and, consequentially, to combat foreign interference in Canada.

Over the past two decades, an increasing number of administrative decisions have involved sensitive information in the context of protecting Canada against threats to national security, including terrorism. In the foreign interference context, it is anticipated that administrative decision-making will involve the use of sensitive intelligence information, for example when making administrative decisions under statutes such as the *Bank Act*.

Creating a fair and comprehensive Secure Review Administrative Proceedings Regime

The Government is seeking views on whether to repeal the existing stand-alone regimes outlined above and seek to amend section 38 of the *Canada Evidence Act* to establish a universally-available Secure Administrative Review Proceedings regime for judicial reviews or statutory appeals in the Federal Courts where sensitive information forms part of the record.

The overarching policy goal would be to provide judges in these proceedings with the authority to consider the entirety of the decision-making record at issue, even where all information therein may not be disclosed to the non-government party, while at the same time providing mechanisms to ensure that the proceeding irrespectively remains fair and effective.

Even though not all situations would engage Charter-protected rights of the affected parties, the key elements and safeguards contributing to procedural fairness could include:

- the inclusion of special counsel;
- the ability to have both open and closed portions of proceedings and rulings;
- a requirement for sufficient disclosure to be made to the affected person, potentially including providing summaries to the affected party that do not reveal the sensitive information itself;
- the same judge would hear section 38 arguments as well as the judicial review or statutory appeal, which would give that judge a better sense of overall fairness; and

- the judge may also, if unable to conduct a fair hearing because all parties are not reasonably informed of the case, make an order granting the party who is not reasonably informed with an appropriate remedy.

Issue 5: Whether to introduce reforms to how national security information is protected and used in criminal proceedings

Context

The challenges discussed in the previous section regarding the protection and use of sensitive information also extends to criminal proceedings. National security information is often used to further a criminal investigation, and at times can be at the heart of criminal charges. It also needs to be protected from unnecessary public disclosure when the disclosure would be harmful.

The challenge is significant in criminal (including foreign interference-related) proceedings involving the defendant's constitutionally protected right to receive full disclosure of the Crown's case, fair trial rights, and the open court principle.

There are fundamental criminal justice, national security, and constitutional issues engaged. For example, to what extent can law enforcement use sensitive and potentially injurious national security information in a police investigation? In addition, if sensitive information is part of the investigative file, how do we ensure that the accused's constitutional rights are fully protected? As discussed above, the *Canada Evidence Act* currently provides a legislative regime governing the disclosure and use in legal proceedings of information that could be injurious to international relations, national defence, or national security. However, there may be opportunities for further improvements.

Consideration is being given to various proposals to address the intelligence and evidence challenges in criminal proceedings, including the following:

Jurisdiction to conduct section 38 *Canada Evidence Act* national security privilege proceedings

Guided by considerations set out in law, the Attorney General of Canada could have the discretion to transfer the authority to make decisions about national security information, from the Federal Court (where these matters are currently evaluated), to a designated judge of the provincial or territorial superior court.

Some of the possible elements could include:

- The establishment of a roster of national security law judges in each provincial and territorial superior trial court.
- The ability of the Attorney General of Canada, once in receipt of a notice under section 38 of the *Canada Evidence Act*, to bring the proceeding to a pre-trial judge or a trial judge seized with the underlying criminal proceeding.

Provide access to special counsel who would protect the interests of the accused

Given the evolving role of security-cleared counsel in the form of amicus in various aspects of *Canada Evidence Act* proceedings, consideration is being given to the creation of a statutory basis for special counsel appointments.

- A judge (Federal Court or provincial or territorial superior court) seized with a section 38 application would have the express authority to appoint a special counsel from a roster to protect the interests of the accused person during the proceeding.
- A designated provincial or territorial superior court judge would have express authority to appoint a special counsel in other non-section 38 criminal proceedings involving national security information (for example, third party records applications and *Garofoli* hearings[6]).
- The special counsel's roles, powers, and obligations would be similar to those set out in sections 85.1 to 85.5 of the *Immigration and Refugee Protection Act*.

Appeals after trials

Currently under the *Canada Evidence Act*, judicial orders of disclosure or non-disclosure made by both the Federal Court and the trial court dealing with information relating to public interest privilege (s. 37) or national security privilege (s. 38) can be appealed while the underlying criminal trial is put on hold. Interlocutory appeals often lead to the possibility of two separate appeals, one in mid trial, and another following a conviction. Such an interlocutory procedure has been criticized, including in the *Ontario Report of the Review of Large and Complex Criminal Case Procedures (2008)* and the *Air India Inquiry (2008)*, as possibly contributing unnecessarily to trial delay. For that reason, the government is considering whether it is desirable and procedurally appropriate to amend

[6] For an explanation of Garofoli applications, please see the discussion below.

sections 37 and 38 of the *Canada Evidence Act* in the context of criminal appeals. These provisions could be amended, as called for in a 2011 resolution passed by the Uniform Law Conference of Canada, to provide that, absent exceptional circumstances with leave of the court of appeal, any decision **not** to disclose specified public interest or national security information, would **only** be reviewable on appeal **after** the conclusion of the trial in the event of a conviction, where the convicted person appeals the decision.

Given that the damage caused by any disclosure of the information is irreparable, the Crown would continue to be able to appeal an order to disclose information on an interlocutory basis. At the conclusion of the trial, the accused would be able to bring two appeals, one of the order regarding disclosure, and the other in relation to any conviction. Conducting the appeal of any non-disclosure order only after the conclusion of the trial would contribute to a better use of court resources and simplify the trial process, and most importantly, could prevent delays that affect the right to having a trial within a reasonable time.

Codify "third party" rules

In criminal proceedings, it is the Crown's obligation to disclose to the accused all information that could "reasonably be used by the accused either in meeting the case for the Crown, advancing a defence or otherwise in making a decision which may affect the conduct of the defence." While the Crown must err on the side of inclusion, it need not produce information that is beyond the control of the prosecution, clearly irrelevant, or privileged. When relevant information is not in the possession of the police or the prosecution – but rather, in the current context, in the holdings of a "third party" like the Canadian Security Intelligence Service (CSIS) or other Canadian national security agencies – an accused person may make an application to assess the existence and relevance of the information pursuant to the two-step common law procedure established in *R. v. O'Connor*.

Some have argued that since CSIS operates independently of the police, its third party status should simply be written into the law, or "codified". Doing so would take away the discretion of the prosecutors and the courts, in assessing how to conduct a trial fairly, to determine whether CSIS was actually acting like a third party in the context of a criminal investigation. Conceivably, there may be instances in the future where CSIS coordinates with law enforcement investigators such that a court would determine that it had joined with the police in conducting

the criminal investigation. For that reason ensuring in law that in all cases CSIS would be considered a third party would not be appropriate.

In an effort to underscore the importance of protecting third party national security information in appropriate cases, and to eliminate trial delays, the Government is currently considering the creation of a statutory test setting out the scope of the disclosure requests which implicate third party government agencies in prosecutions of designated national security offences. Such a change to the criminal law would at all times respect the Charter rights of the accused to full answer and defence.

Outside of the section 38 reforms, a new rule for records in the hands of a third party would apply when national security information is alleged to be held by a government institution:

- Defence counsel would be required to apply, in writing, for a third party disclosure order, where they believe that the information exists, is in the possession or control of the third party entity, and that the information sought would be "likely relevant" to an issue at trial.
- After determining that the above criteria are met, the judge could require that the third party supply a copy of the information, or a summary, for review.
- After reviewing the information or summary, the judge would be required to assess and weigh certain factors, including the fair trial rights of the accused and the impact of any potential disclosure order upon the third party entity (for example, CSIS).
- There would be the potential for appointing a special counsel to protect the interests of the accused in any proceedings where defence counsel are excluded. However, the goal would be to create a mechanism that prevents the triggering of the process in section 38 of the *Canada Evidence Act*, and not to duplicate that procedure.
- At all times, the court would need to ensure that its decision of whether to order the disclosure of third party records respects the fair trial rights of the accused.

Sealing Orders under the Criminal Code

Section 487.3 of the *Criminal Code* deals with orders that deny access to information relating to information presented to a judge in support of the issuance of a warrant. The provision prohibits, on application at the time the

warrant is sought, access to search warrant-related documentation to which the public would otherwise have a right of access, on the ground that the ends of justice could be subverted by its disclosure.

The Government is currently considering an amendment to provide a specific national security consideration to this process.

Currently, subsection 487.3(2) lists several factors that a judge can consider when determining whether to make an order denying access to information. The list of factors could be expanded to provide that a judge may issue an order denying access to and disclosure of information where the disclosure of information would be injurious to international relations, national defence or national security.

- Where the order is made, all documents relating to the application would be sealed, subject to any terms and conditions that the judge considers appropriate in the circumstances. For example, a judge in granting such an order could indicate that the order is in place for a specific period of time.

New rules governing Garofoli applications

When the evidence against an accused at a criminal trial includes information obtained from a wiretap or search warrant, the accused's lawyer may try to have that information excluded from the trial through a procedure called a *Garofoli* application, brought before the trial judge. A *Garofoli* application seeks to protect the rights of an accused person by ensuring that the evidence admitted at trial was obtained lawfully and in accordance with Charter-protected rights, such as the right to be free from unreasonable search and seizure.

A *Garofoli* review by a judge does not determine whether the allegations underlying the wiretap application are true – this a matter to be decided at trial – but rather whether the police had a reasonable belief in the existence of the grounds needed to apply for the search warrant or authorization. What matters, for the purpose of the *Garofoli* review, is what the police affiant knew or ought to have known at the time the affidavit in support of the wiretap authorization was sworn.

As a general rule, there are two ways to challenge a wiretap authorization in these proceedings: first, that the record before the authorizing judge was insufficient to meet the requirements in the *Criminal Code* that police must meet to obtain the authorization; second, that the record before the judge who authorized the

warrant or wiretap did not accurately reflect what the affiant knew or ought to have known, and that if it had, the authorization could not have issued.

In situations where the warrant or wiretap was authorized, relying, even to a small extent, upon national security information, the determination of the national security privilege in the context of a *Garofoli* application presents difficult procedural challenges in terms of the protection of information from public disclosure and the fairness of the proceedings. The challenge is in ensuring that law enforcement investigations can proceed – even when they rely in part on sensitive national security information – while ensuring a fair process for an accused to challenge warrants based on that information. It is for that reason that the Government is currently examining the possibility of creating special procedures for a trial court to review and assess sensitive national security information when an accused challenges a *Criminal Code* warrant that was issued on the basis of that sensitive information.

What do you think?

1. Do you see benefits to the criminal proposals in the investigation and prosecution of foreign interference cases?
2. Do the proposals strike the right balance between protection of information and fundamental rights and freedoms protected by the *Charter of Rights and Freedoms*?
3. Are there other intelligence and evidence related measures that would assist in this regard?