Our Security, Our Rights

National Security Green Paper, 2016

Background Document




This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Government of Canada
Gouvernement du Canada

Canada

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Our Security, Our Rights: National Security Green Paper, 2016

BACKGROUND DOCUMENT

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

CONTENTS

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

INTRODUCTION

Setting the Scene

Canada has long dealt with terrorism threats from a diverse set of groups. Some threats resulted in tragic terrorist attacks. For example, a terrorist bomb exploded aboard Air India Flight 182 in 1985, killing 329 passengers and crew. In a related incident, a second bomb exploded at Narita airport in Japan, killing two more individuals. This remains the worst terrorist attack in Canadian history.

Following the September 11, 2001 attacks in the United States (U.S.), Canada enacted the *Anti-terrorism Act*. The Act recognized the unique nature of terrorism and created offences addressing specific aspects of terrorism. These offences included contributing to the activities of a terrorist group, instructing someone to carry out a terrorist activity, and harbouring a terrorist.

Since 2001, threats to Canadian and international security have continued to evolve. Groups inspired by al-Qaida have emerged in many parts of the world. In early 2014, one of these groups, al-Qaida in Iraq, severed ties with al-Qaida and emerged anew as the Islamic State of Iraq and the Levant (ISIL). What has been referred to as ISIL will be referred to as Daesh in this document. Since the start of the Syrian conflict in 2011, many Canadians have travelled to Syria and Iraq to join Daesh's predecessor and then Daesh itself. Daesh's declaration of a "caliphate" led to even more of these "extremist travellers" from Canada joining Daesh abroad. Some later returned to Canada, leaving trained and connected terrorist actors in our presence. The return of travellers can result in the presence of trained and connected terrorist actors within Canada.

Extremist narratives have also inspired some Canadians to plot and pursue attacks. Sometimes their targets are domestic, such as the 2014 attacks in Ottawa and Saint-Jean-sur-Richelieu. Other times, their targets are outside Canada, such as the Algerian gas plant attacked by terrorists, including two Canadians, in 2013.

The Minister of Public Safety and Emergency Preparedness recently released the *2016 Public Report on the Terrorist Threat to Canada*. The Report noted that the principal terrorist threat to Canada remains that posed by violent extremists who could be inspired to carry out an attack within Canada. Violent extremist ideologies espoused by terrorist groups like Daesh and al-Qaida continue to appeal to certain individuals in Canada.

Both the threat of terrorism and the counter-terrorism tools we use to respond have evolved over the years. However, there has been one constant imperative from the Government of Canada's perspective. That is to ensure that any actions by the Government respect Canadian values, including the rights and freedoms guaranteed by the *Charter*, as well as equality and multiculturalism.

National security institutions in Canada are professional, responsible and effective in the work they do. They work within a well-defined set of legal authorities and respect Canadian law. Their core

duty is to keep Canadians safe—and they do so daily. National security institutions in Canada are subject to measures that make them accountable. These accountability measures ensure that these institutions are acting within the law and are being effective. Accountability for national security institutions is, therefore, an important part of any discussion on national security, as it offers protections and safeguards.

The Government is aware that its actions in security matters can impact rights. In protecting national security, the Government must find an appropriate balance between the actions it takes to keep Canadians safe and the impact of those actions on the rights we cherish. The question is: what is an appropriate and reasonable impact?

The Canadian public, stakeholders, experts and those in government institutions will have a variety of views on what constitutes an appropriate balance. Canadians rightly expect strong justifications to limits their rights. This means that we must look at measures to protect national security to see whether they are effective, if there are potential alternatives and if they have properly taken into account the rights they affect.

Human Rights

Canada is founded upon the rule of law, of which the Constitution is the "supreme law." This means that all laws enacted by Parliament and all actions taken by the Government of Canada must be consistent with the Constitution, which includes the *Charter*. The *Charter* reflects our basic values and guarantees our fundamental rights and freedoms, including freedom of expression and association, and the rights to equality, privacy, and the presumption of innocence. The purpose of the *Charter* is to ensure that we are governed in accordance with our basic values. Any laws of Parliament and actions of government that are inconsistent with the *Charter* are unconstitutional and can be declared so by the courts.

The rights and freedoms guaranteed in the *Charter* are not absolute. They can be limited in accordance with the law, if justifiable. Justifiable limitations are generally those that pursue important objectives and that impact rights or freedoms as little as reasonably possible in the circumstances. Also, limitations are only justifiable if, overall, the benefits from these limitations outweigh the harm to the right.

This concern for balance is acutely important in the national security context, where *Charter* rights and freedoms regularly come into play. Measures to protect national security are aimed at fulfilling the Government's primary mandate, which is to safeguard the people, institutions and values of Canada. Preserving national security includes protecting what defines Canada, including democracy, multiculturalism, and respect for the rule of law and fundamental rights and freedoms.

The *Charter* establishes a minimum standard of conduct by governments in Canada. Governments are free to produce legislation or policies, or carry out activities, that give greater protection to rights

and freedoms than the *Charter* requires. In some cases, the appropriate balance between national security concerns and *Charter* rights may result in greater protection. The Government is interested in the views of Canadians about when it may be appropriate in national security matters to give greater protection to rights and freedoms than that required by the *Charter*.

Privacy

In recent years, many countries have experienced high-profile public controversies about privacy impacts of national security activities.

It is difficult to hold an informed public debate about whether privacy impacts are appropriate. In part, this is because revealing some details about national security operations can undermine their effectiveness.

That said, effective and sustainable anti-terrorism measures should reflect a robust democratic consensus, at least at the level of principles. In matters involving privacy in particular, it might not be enough to achieve that consensus if anti-terrorism activities merely satisfy the minimum constitutional and legal standards. The Government is interested in the views of Canadians to help determine where the consensus lies.

Consultation Process

How best to respond to terrorism while protecting rights and freedoms is a highly complex issue. As the Government examines possible changes to Canada's counter-terrorism framework, it is asking Canadians to become active partners in finding an appropriate balance between security and rights. These consultations will help the Government develop more informed policies in this complex area.

Each chapter of this background document provides information on applicable laws, issues, challenges and potential impacts on rights in the counter-terrorism context. It contains hypothetical scenarios to better illustrate the concepts being presented.

All Canadians are invited to respond online at **Canada.ca/national-security-consultation** to the issues raised in the Green Paper and this background document. Responses will be accepted until December 1, 2016.

The Government will consider the responses and use them to help develop any new laws and policies. The Government will also keep Canadians up to date on the progress of consultations.

Hypothetical scenarios will be presented throughout this document to illustrate issues. The roles of the characters used in these scenarios are set out in the Annex.

This Green Paper is intended to prompt discussion and debate about Canada's national security framework, which will inform policy changes that will be made following the consultation process.

Our main scenario starts as follows…

Mr. A is a charismatic speaker who holds weekly meetings in a local community centre. He has strong views on social and political issues. He invites individuals with similar interests to attend. Some of these individuals have become friends with each other, and with Mr. A. They are also his most devoted followers.

Mr. A believes that things in Canada need to change. He is looking for people who are willing to get involved and make this happen. Over time, his calls for political and social change start taking on a more violent tone.

ACCOUNTABILITY

Some government agencies have unique intelligence collection and enforcement powers to protect national security. They must exercise these powers according to specific laws and in a manner consistent with the *Charter*. These powers are potentially intrusive, and can impact rights and freedoms. For this reason, these powers must be exercised with great care.

Much work of these agencies occurs in secret. This is because the public disclosure of sensitive information could harm national security by putting investigations, sources of information and investigative techniques at risk. As a result, effective accountability mechanisms are key to maintaining the public's trust in these agencies. Accountability mechanisms provide assurance that agencies act responsibly, strictly within the law and with respect for Canadians' rights and freedoms.

Ministerial Oversight

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence have important responsibilities with regard to the national security and intelligence agencies in their respective portfolios.

The Minister of Public Safety and Emergency Preparedness is responsible for three national security agencies: the Canada Border Services Agency (CBSA), CSIS and the Royal Canadian Mounted Police (RCMP). The Minister is also responsible for Public Safety Canada.

The Minister of National Defence is responsible for the Communications Security Establishment (CSE), the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

The Ministers are accountable to Parliament for the activities of their respective agencies.

If the activities of CSE or of CSIS employees are believed to have contravened the law, the minister responsible for the relevant agency is engaged and the Attorney General of Canada is informed.[1]

Ministers can issue formal directions that establish guidelines on the conduct and management of operations, although the principle of police independence limits direct ministerial involvement in day-to-day law enforcement operations. Ministerial Directions (MDs) may also specify reporting requirements and procedures for obtaining approval for agency activities.

A number of MDs are currently in effect for the CBSA, CSE, CSIS and the RCMP. For example, in 2015, CSIS was issued wide-ranging new MD on operations and accountability. The RCMP is also

[1] In the case of CSE, it is the CSE Commissioner who informs the Minister and Attorney General of Canada. Reports to the Attorney General of Canada about CSIS employees must also be provided to the Security Intelligence Review Committee.

subject to several MDs that provide guidance on aspects of national security investigations related to sensitive sectors, accountability, and cooperation. MDs on information sharing with foreign entities have also been issued to the CBSA, CSE, CSIS and the RCMP. These MDs established a consistent process for deciding whether to share information with foreign entities where there may be a risk of mistreatment stemming from the sharing of information, in accordance with Canada's laws and legal obligations.

The Judiciary

Courts are involved in national security matters in several ways. Judges decide whether to issue warrants for CSIS and law enforcement agencies to use intrusive powers when investigating threats. Judges ensure that agencies meet the legal requirements to obtain warrants and that the warrants comply with the *Charter*. Judges also have the discretion to include in warrants any terms and conditions that are advisable in the public interest. For example, a judge might limit how long a government institution can keep the information it obtains.

More generally, judges decide whether activities leading to an individual's arrest and criminal prosecution are justifiable and proper. For example, judges examine whether investigators respected constitutional rights during investigations and whether evidence was properly collected and should be admitted at trial. Judges also have the authority to provide remedies to citizens who show law enforcement misconduct.

The Federal Court may also hear applications for judicial review of administrative decisions made by the Government in national security matters. Judicial review is a process by which the courts ensure that government decisions were fair and complied with the law. For example, the Court could review decisions made under national security programs such as the Passenger Protect Program.

Independent Review

Canada has a long-standing system of independent, non-partisan bodies reviewing the activities of certain agencies that deal with national security matters. Review bodies operate at arm's-length from government. Their main task is to ensure that national security and intelligence agencies comply with the law and MDs.

At present, there are three such bodies:

- the Civilian Review and Complaints Commission (CRCC), responsible for reviewing RCMP activities;
- the Security Intelligence Review Committee (SIRC), responsible for reviewing CSIS activities; and

- the Office of the Communications Security Establishment Commissioner (OCSEC), responsible for reviewing CSE activities.

Governor-in-Council (Cabinet) appointees head the CRCC and SIRC. The Governor-in-Council appoints a supernumerary judge or retired judge of a superior court to head OCSEC. Each review body has an independent research staff and legal counsel to help it.

All three review bodies have a mandate to review the activities of, and hear complaints against, the particular agency for which they are responsible. They have access to information held by the agency. Each review body produces a public report every year summarizing its activities, including findings and recommendations from reviews and complaints.

The authority of these three review bodies does not extend beyond the specific agency for which each review body is responsible. As a result, review bodies do not share classified information with each other or conduct joint reviews of national security and intelligence activities.

Parliament

Parliament has several roles in national security matters. It holds ministers to account for the actions of the institutions for which they are responsible. Parliament reviews, refines and enacts proposed legislation on national security matters. This process often involves calling witnesses to provide expert evidence about the issues raised by the proposed legislation.

Some laws contain provisions requiring a review of the law after a set period. For example, the Government has made a commitment to require a review of the ATA, 2015 after three years. Some laws might also require that a provision expires on a set date unless renewed. Other laws may require an annual report about the use of a particular provision.

House of Commons and Senate committees can also examine national security policy issues and conduct studies of government activities and existing legislation.

Normally, however, parliamentarians do not see classified information. This limits their ability to examine national security issues in depth. To resolve this, the Government has tabled a Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*[2] to create a national security and intelligence committee of parliamentarians with broad access to classified information. The committee would examine how institutions are working together to keep Canadians safe from national security threats. It would also seek to ensure that institutions comply with Canada's laws and respect fundamental values, the democratic nature of our open society and the rights and freedoms of Canadians.

[2] Bill C-22 can be accessed at:

http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=8375614

Agents of Parliament

Certain agents of Parliament scrutinize the national security activities of all federal institutions in relation to their specific mandates. For example, the Privacy Commissioner of Canada can examine their handling of personal information. The Privacy Commissioner also has a mandate to review the operations of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) every two years. The Information Commissioner of Canada investigates complaints about the Government's handling of access to information requests. The Auditor General (AG) can conduct "value-for-money" audits of national security programs. [3]

Commissions of Inquiry

Commissions of inquiry provide another means to keep government institutions accountable. Commissions of inquiry are "established by the Governor in Council (Cabinet) to fully and impartially investigate issues of national importance."[4] Within the last decade, the O'Connor, Iacobucci and Major Commissions[5] each reported on the activities of various national security institutions. Many, but not all, of their recommendations have been implemented. For example, Commissioner O'Connor made a number of detailed recommendations for changes to the framework for national security accountability in Canada that have not been implemented.

[3] For example, in spring 2013, the AG reported on its audit of government spending on the Public Security and Anti-Terrorism Initiative; in fall 2012, the AG reported on the Government's efforts to protect Canadian critical infrastructure against cyber threats; and in March 2009, the AG reported on intelligence and information sharing in relation to national security.

[4] Privy Council Office, Commissions of Inquiry.

[5] Specifically, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (report released September 18, 2006); the Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (report released 22 October 2008); and the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (report released 17 June 2010).

What are other countries doing?

Some of our closest allies, including Australia and the United Kingdom (UK), share democratic traditions and institutions. As such, their experiences ensuring the accountability of national security and intelligence services are useful to consider when reflecting on Canada's own accountability mechanisms.

For instance, both Australia and the UK have parliamentary committees with access to classified information dedicated to national security. Indeed, the UK's Intelligence and Security Committee can, with the government's consent, review specific national security operations.

Australia and the UK also take different approaches to independent review of national security activities. In the UK, a number of different commissioners concentrate on a specific aspect of national security and intelligence across a range of agencies. These include:

- The Interception of Communications Commissioner ensures the propriety of communications interception activities;
- The Intelligence Service Commissioner's Office and the Office of Surveillance Commissioners review covert surveillance activities other than communications intercepts; and
- The Investigatory Powers Tribunal hears complaints and can authorize compensation and other redress.

The UK's system may change shortly, however; the *Investigatory Powers Bill*, currently before the UK Parliament, would consolidate the current bodies into a single Investigatory Powers Commission, and would also establish Judicial Commissioners charged with approving warrants.

Australia, for its part, has long had a consolidated model. There, the Inspector General of Intelligence and Security reviews all key intelligence and security agencies for compliance with the law, ministerial directives, and in regard to human rights.

In addition to its commissions and tribunals, the UK's Independent Reviewer of Terrorism Legislation provides expert commentary on proposed legislation, and reviews the use of powers granted by certain key pieces of existing legislation. In carrying out these duties, the Reviewer – who is appointed from outside of government – has access to classified information. Australia has a similar mechanism, the Independent National Security Legislation Monitor, which reviews, on an ongoing basis, national security and counter-terrorism legislation.

What do you think?

Should existing review bodies – CRCC, OCSEC and SIRC – have greater capacity to review and investigate complaints against their respective agencies?

Should the existing review bodies be permitted to collaborate on reviews?

Should the Government introduce independent review mechanisms of other departments and agencies that have national security responsibilities, such as the CBSA?

The proposed committee of parliamentarians will have a broad mandate to examine the national security and intelligence activities of all departments and agencies. In addition to this, is there a need for an independent review body to look at national security activities across government, as Commissioner O'Connor recommended?

The Government has made a commitment to require a statutory review of the ATA, 2015 after three years. Are other measures needed to increase parliamentary accountability for this legislation?

PREVENTION

A new phrase has appeared in the Canadian lexicon: radicalization to violence. Radicalization to violence is a process where people take up an ideological position that moves them towards extremism and ultimately, terrorist activity.

Semantics are important here. It is not a crime to be a radical. Throughout history, change has been brought about by individuals whose radical ideas have inspired new ways of thinking. What is a crime is terrorism – violence committed in the name of radical ideologies or beliefs. As a Government, as a society, we are obliged to respond to criminal violence, whatever form it takes.

When someone decides to use violence to reach a political, ideological or religious goal, they have "radicalized to violence." This is where terrorism takes root. This person may be formally linked to a terrorist group, inspired by a terrorist group, or radicalized to violence through their own beliefs. The question is, how does radicalization to violence begin? And, more important, what can be done to prevent it?

What Plays a Role?

We know that specific "narratives" drive radicalization to violence. These narratives reduce an individual's understanding of global events to a few simplistic propositions. Radicalization is also a social process occurring within networks and communities, both virtual and physical. People can be influenced by friends, mentors and other individuals in their lives.

Associating with others ascribing to violent radical ideologies can influence individuals to move further down the path of radicalization to violence. For example, it is no accident that many people who become extremist travellers – individuals who go abroad to join or contribute to terrorist groups – know others like them who have gone abroad. Some extremist travellers who return to Canada have the experience to plan and carry out terrorist attacks at home, as well as the credibility to recruit, encourage, mentor and facilitate the actions of aspiring terrorists.

The Internet also plays an important role in radicalization to violence. Terrorist groups use websites, chat rooms and social media as key propaganda and recruitment tools. For example, in the conflict in Iraq and Syria, some individuals and groups regularly post content and video clips on social media. These online posts boast of battlefield victories and seek to justify terrorist attacks and recruit young people from around the globe to join the fight.

Consider a scenario…

Mr. B is 17 years old and in his final year of high school. He was born and raised in a large suburban area. His neighbours think he is polite and he has no criminal record. Several months ago, a friend encouraged Mr. B to attend weekly discussion group meetings hosted by Mr. A. His charisma, moving speeches about global politics and self-confidence immediately drew in Mr. B. Over time, Mr. A's extremist views and promotion of violence began to resonate with Mr. B.

Between weekly meetings, Mr. B now spends much of his time on the family computer, watching violent videos that Mr. A has posted online. Some friends have noticed changes in Mr. B's behaviour and that he spends more time alone than before. Some teachers have noticed that he is less engaged in the classroom and intolerant of the views of his peers during class discussions. His association with Mr. A worries Mr. B's parents, but their attempts to talk to him about it have failed. They want to know what they can do and where they can go for help to prevent their son from becoming fully committed to a violent radical ideology.

What Can be Done?

All levels of government, communities and other stakeholders must work together to steer at-risk individuals away from radicalization to violence. They also need to give at-risk individuals the support they need to choose an alternative path that reflects Canadian values of peace and acceptance.

Law enforcement organizations play an important role. They seek to support individuals at risk of radicalization to violence and respond if individuals progress to criminal activities. The RCMP train law enforcement officers and front-line personnel to recognize early warning signs and lead interventions to divert individuals from the path of radicalization to violence. As well, Correctional Services Canada conducts tailored interventions for inmates who have radicalized to violence or who are at risk of doing so.

Family members, friends and others close to at-risk individuals can also play a key role in countering radicalization to violence. They are often aware of the individual's beliefs and intentions. Individuals who are early on in the process of radicalization may have many questions and doubts. At this early stage, it may be possible to steer individuals away from radicalization to violence. For this reason, it is essential to support local communities to address this issue.

National Leadership

The Government is also exploring new ideas and innovative approaches to counter radicalization to violence. Budget 2016 announced $35 million over five years, with $10 million per year ongoing, to create an Office of the community outreach and counter-radicalization coordinator. The Office will

lead Canada's response to radicalization to violence, coordinate federal, provincial, territorial and international initiatives, and support community outreach and research. The material immediately below describes in greater detail what the Office could do.

Work with Communities

The most effective way to prevent radicalization to violence often lies within communities. It involves working with local leaders to develop early intervention programs. A key focus for the new Office is to reach out to Canadians and build constructive relationships with communities across Canada, raise general awareness about threats and means to address them, and maintain a continual dialogue with those communities.

Engaging with Canadians will help identify priorities for the Office and inform the development of a national strategy to counter radicalization to violence. The Office is seeking to support programs that focus on individuals at risk of radicalization to violence. These programs can include community capacity-building, mentorship, multi-agency interventions and training and support for those involved in front-line intervention work (such as youth workers, corrections and parole officers, social service providers, faith leaders and mental health practitioners).

The City of Montreal is also working in this area. It has established a Centre for the Prevention of Radicalization Leading to Violence. The Centre brings together partners from various sectors, including health and social services, public safety and education. The goal is to develop expertise, define areas of prevention and intervention, and empower communities to address radicalization to violence. The Office can incorporate lessons learned from Montreal's experience into future programming.

Engage Youth and Women

Radicalization to violence in Canada affects young people disproportionately. Engaging with youth is therefore important in addressing this issue. Early in the process of radicalization they may have many questions and doubts. They turn to the guidance that is available. At this early stage, tailored outreach has the potential to steer at-risk youth away from radicalization to violence. The Office is looking to start a positive conversation with young people, raise their awareness about the dangers of becoming radicalized to violence, and empower them to respond to the issue.

Women can play a key role in this area. Research has shown that the involvement of women – in different capacities and roles, in both the private and public spheres – is essential to effective prevention efforts. As gatekeepers to their communities, they are often well-positioned to serve as credible, resonant voices against violent radical ideologies. The Office can support local initiatives that engage, inform and empower women to better identify and address violent radicalization in their families and communities. The Office can also develop and share tools, resources and information to support women – and men – in responding to this issue.

Promote Alternative Narratives

Terrorist groups often aim to influence potential recruits by promoting and spreading certain messages. Promoting positive, alternative narratives is one way to counter such messages.

The Office is looking for ways to support credible voices and empower community actors—particularly youth and women —to develop programs, messaging or other tools that reflect local realities. These measures can be used to challenge violent radical narratives and promote critical thinking. For example, terrorist groups use the Internet and social media to spread violent radical ideologies and messaging quickly and broadly. The Office can support programs that harness these tools for positive uses.

Foster Research

Research is a key element in countering radicalization to violence. It can inform policy development, improve the design of programs and tools, and help identify appropriate and effective ways to counter radicalization to violence. The Government is looking to engage with academics, think tanks and others to determine research priorities, identify best practices and lessons learned and develop effective tools to measure the success of programs.

Through the Kanishka Project[6], the Government has invested in research about radicalization to violence and has identified a number of best practices. There is more to learn, and the demand for that information and research is great. Support for action-oriented research is important. Such research produces guides, tools and other resources to assist the public, as well as mechanisms to evaluate programs and measure their success. Evaluation tools will help develop more effective programs to counter radicalization to violence. Knowing what works will also inform policies and priorities, and can contribute to the success of Canada's overall approach to the issue.

What are other countries doing?

Countering radicalization to violence is a priority for the international community. The United Nations emphasized the importance of prevention efforts in United Nations Security Council Resolution 2178, which was unanimously adopted in September 2014. Also, in January 2016, the United Nations Secretary-General released a Plan of Action to Prevent Violent Extremism, which encourages countries to develop national strategies for addressing radicalization to violence. Canada strongly supports this initiative.

[6] http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/r-nd-flght-182/knshk/index-en.aspx

Like Canada, other countries have begun to develop policies and programs to respond to this issue. Working with communities, engaging youth and women, promoting alternative narratives, and conducting research are also key areas of focus for our international partners.

Examples

Community engagement is a cornerstone of a number of countries' national strategies to counter radicalization to violence. For example, to enhance social cohesion and harmony, Singapore's Community Engagement Programme brings together Singaporeans from different communities – from religious groups, to unions, to educational institutions, to the media – to strengthen inter-communal bonds, build partnerships and enhance social resilience. Also, to better inform citizens on radicalization to violence, Australia has created a website called Living Safe Together as a central online location where people can read about how Australia addresses this issue, seek information and advice on radicalization to violence, and access other resources. The Office could develop similar initiatives that are tailored to the Canadian experience.

Some countries have also explored programs focusing on youth. For example, in Sweden, there is a youth centre called "Fryshust" that promotes confidence, responsibility, and understanding to enable young people to develop their innate abilities and find their way in society. Also, in Denmark, an organization called "My House" aims to pair individuals at risk of radicalization to violence with mentors that face similar challenges and come from similar backgrounds, but that can show an alternative, positive path to explore.

Finally, engaging women in prevention efforts is an important element of some countries' approaches to this issue. For example, in the UK, "Project Shanaz" was developed in 2011 to understand the perception women have of activities related to the country's national strategy to counter radicalization to violence. This project led to the establishment of the Shanaz Network, an independent body of 50 women community leaders that contributes to the development of policies and strategies related to radicalization to violence. A similar model in Canada could help inform the development of a new strategy to counter radicalization to violence.

What do you think?

The Government would like your views about what shape a national strategy to counter radicalization to violence should take. In particular, it is looking to identify policy, research and program priorities for the Office of the community outreach and counter-radicalization coordinator. What should the priorities be for the national strategy?

What should the role of the Government be in efforts to counter radicalization to violence?

Research and experience has shown that working with communities is the most effective way to prevent radicalization to violence. How can the Government best work with communities? How can tensions between security concerns and prevention efforts be managed?

Efforts to counter radicalization to violence cannot be "one size fits all." Different communities have different needs and priorities. How can the Office identify and address these particular needs? What should be the priorities in funding efforts to counter radicalization to violence?

Radicalization to violence is a complex, evolving issue. It is important for research to keep pace. Which areas of research should receive priority? What further research do you think is necessary?

What information and other tools do you need to help you prevent and respond to radicalization to violence in your community?

THREAT REDUCTION

Since its creation in 1984, CSIS has collected information and intelligence on threats to the security of Canada, at home and abroad.[7] CSIS uses the information to advise other institutions of government, such as law enforcement, about these threats. These institutions then in turn act on the information.

The ATA, 2015 amended the *Canadian Security Intelligence Service Act* (*CSIS Act*) to authorize CSIS to reduce threats to the security of Canada. CSIS can now do more than share information. It can also take direct action against threats to reduce the danger they pose. Threat reduction (also called disruption) seeks to prevent or discourage people who pose a threat from carrying out their plans.

The threats facing Canada have evolved significantly in recent years. In part, this flows from the trend away from complex terrorist operations towards loosely organized small-scale attacks, the growing use of the Internet and mobile communications, and the ease with which people can move about the globe. These changes have made it harder for security agencies to prevent attacks.

The RCMP have long had a crime prevention mandate. This allows them to act pre-emptively to prevent threats from materializing. However, there are differences in the roles and responsibilities of CSIS and the RCMP. These include different priorities, different approaches, access to different information and a different international presence. For these reasons, during the development of the ATA, 2015, it was felt that there were situations where CSIS was best placed to take timely action to reduce threats. Even before the debate about the ATA, 2015, a threat reduction mandate for CSIS was being discussed. A 2010 report by SIRC recommended that CSIS seek guidance and direction on the issue of threat reduction. In 2011, the Senate Special Committee on Anti-terrorism also considered threat reduction and issued recommendations.

The CSIS threat reduction mandate does not give it law enforcement powers. For instance, CSIS cannot arrest individuals. CSIS continues to work in consultation with the RCMP and other law enforcement agencies.

The Threat Reduction Mandate

For some threat reduction measures CSIS requires a warrant from the Federal Court. Whether a warrant is needed hinges on whether the proposed actions by CSIS would affect *Charter* rights or would, without a warrant, be against the law.

---

[7] "Threats to the security of Canada" are defined in section 2 of the *CSIS Act*, and encompass terrorism (or more precisely "acts of serious violence… for the purpose of achieving a political, religious or ideological objective"), espionage and sabotage, foreign-influenced activities that are clandestine, deceptive, or threaten a person, as well as domestic subversion aimed at the overthrow by violence of the constitutional order of government. Lawful advocacy, protest and dissent are excluded, unless carried out in conjunction with any of the activities referred to above.

Consider a scenario where a warrant is not needed…

Mr. C, a Canadian citizen, attends Mr. A's weekly meetings. He has even voiced support for terrorist activity in Canada in response to terrorist propaganda encouraging attacks in the West. Mr. C is seeking employment as a guard for a firm that provides security at major concerts and other events. CSIS approaches the firm and provides information about Mr. C. Once aware of Mr. C's support for terrorist activity, the firm launches an investigation and decides to restrict Mr. C's work. As a result, Mr. C does not gain privileged access to major events where he could pose a security threat.

Consider a scenario where a warrant is needed…

Mr. D, an associate of Mr. A, is promoting extremism on his personal website by posting videos supporting a terrorist group. His website is hosted outside Canada and also includes how-to guides for making bombs and suicide vests. CSIS obtains a threat reduction warrant from the Federal Court allowing it to modify the website's how-to guides. CSIS replaces some of the terrorism-related details with misinformation that will make the devices fail. Mr. D and his followers do not notice the changes. As a result, their effective support to terrorism has been limited.

The table below sets out the differences between threat reduction measures by CSIS that require a warrant and those that do not.

	No warrant required	**Warrant required**
Examples	– Interviews – Asking friends to intervene – Reporting extremist content to social media providers	– Disrupting financial transactions – Interfering with terrorist communications – Manipulating goods intended for terrorist use
Procedure CSIS must follow to take threat reduction measures	– CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada – CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances – CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate	– CSIS must have reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada – CSIS must demonstrate that the proposed measure is reasonable and proportional in the circumstances – CSIS must obtain internal approval, perform a risk assessment, and consult law enforcement and other agencies as appropriate – **CSIS must obtain approval from the Minister of Public Safety and Emergency Preparedness for a warrant application** – **The Federal Court then reviews the warrant application and decides whether to issue the warrant**

Threat reduction measures that would cause death or bodily harm, violate a person's sexual integrity or interfere in the course of justice are prohibited.[8]

[8] See *CSIS Act*, section 12.2.

Potential Impacts on *Charter* Rights

Threat reduction measures may affect Canadians' *Charter* rights and freedoms, depending on the circumstances of the measure.

CSIS must obtain a warrant from the Federal Court before it can take threat reduction measures that would affect rights protected under the *Charter*. The *Charter* recognizes that rights and freedoms are not absolute and that at times they may justifiably be limited. A warrant shows that the Court has determined in advance that the proposed threat reduction measures are reasonable and proportional in the circumstances.

Warrants have long been used to balance government objectives and *Charter* rights. Since 1984, CSIS has sought warrants from the Federal Court to collect intelligence using techniques that limit privacy rights protected by section 8 of the *Charter*. Police wiretaps and search warrants work in a similar way. Threat reduction warrants are a departure from previous warrant regimes. They can limit additional *Charter* rights, not just privacy rights under section 8.

What are other countries doing?

Intelligence and security services in many of Canada's allies have the mandate to reduce threats to national security and a range of threat reduction powers. There is no standard approach to threat reduction, however, as each country has a unique system of government, making direct comparisons difficult. In some countries, responsibility for national security and intelligence is divided between foreign and domestic services. In others, responsibility is divided between intelligence and law enforcement. In the U.S., for example, there are distinct domestic and international agencies. Domestically, the FBI has both intelligence and law enforcement responsibilities.

Nonetheless, various allied intelligence and security services have the authority to take direct action against threats, domestically and/or abroad, subject to various limitations. In the UK, for instance, the Security Service (also known as MI5) has legal authority to take action to protect national security, including against the threat of terrorism. The Australian Secret Intelligence Service has a broad mandate to undertake "other activities", including threat reduction measures outside of Australia. French authorities can also disrupt threats to France and French interests abroad.

Internationally, the means by which threat reduction activity is legally authorized takes various forms. Canada's framework requires court warrants for measures that would affect *Charter* rights. In other countries, senior members of the executive branch authorize intrusive threat reduction measures.

In the current international environment, the threat reduction mandate allows CSIS to contribute to a broader range of allied operations against terrorism and other shared threats than was previously the case.

What do you think?

The Government wants to know what you think about CSIS's new threat reduction mandate:

CSIS's threat reduction mandate was the subject of extensive public debate during the passage of Bill C-51, which became the ATA, 2015. Given the nature of the threats facing Canada, what scope should CSIS have to reduce these threats?

Are the safeguards around CSIS's threat reduction powers sufficient to ensure that CSIS uses them responsibly and effectively? If current safeguards are not sufficient, what additional safeguards are needed?

The Government has committed to ensuring that all CSIS activities comply with the *Charter*. Should subsection 12.1(3) of the *CSIS Act*[9] be amended to make it clear that CSIS warrants can never violate the *Charter*? What alternatives might the Government consider?

[9] Subsection 12.1(3) of the Act states that CSIS "shall not take measures to reduce a threat to the security of Canada if those measures will contravene a right or freedom guaranteed by the *Canadian Charter of Rights and Freedoms* or will be contrary to other Canadian law, unless [CSIS] is authorized to take them by a warrant…."

DOMESTIC NATIONAL SECURITY INFORMATION SHARING

National security institutions need information to detect, analyze, investigate and prevent threats. It often takes multiple pieces of information to provide a complete threat picture, and today's national security threats can evolve rapidly, heightening the need for timely and complete information.

Yet information needed for national security purposes can be held in different places by various institutions of government. Because of this, the sharing of information is an important part of national security work today. The report of the Air India inquiry[10] stressed this point. The report of the O'Connor inquiry[11] also mentioned the importance of information sharing for investigations and prevention of national security threats, but also highlighted the need for caution with respect to the content of the information and its use by the recipient.

Federal institutions with national security responsibilities can collect information to carry out lawful duties and responsibilities. This collection may be authorized by an Act of Parliament, the common law or the Crown Prerogative. Even institutions that do not have a national security mandate (such as the Department of Fisheries and Oceans) sometimes hold information that could be important for national security institutions. Non-national security institutions must be able to disclose that information to institutions that have a mandate to act on it.

Government institutions must follow certain rules when sharing information, especially information about individuals. These rules are important to protect privacy rights. However, their complexity can sometimes make it difficult to know whether a given institution is permitted to share information. This can prevent information from getting to the right institution in time.

The *Privacy Act*

The *Privacy Act* protects individuals' personal information by regulating how federal government institutions collect, use, retain and disclose it. The Act limits the collection of personal information by government institutions to that which relates directly to their work. It also limits when this information can be used and disclosed without the consent of the individual to whom it relates.

The *Privacy Act* recognizes that personal information may be disclosed without consent in some situations, including those involving national security. The main exceptions to the rule preventing disclosure without consent are as follows:

1. "Consistent use": One federal institution may share information with another institution for the purpose for which the information was collected or for a use consistent with that purpose (for an example, see the scenario below).

2. "Investigative bodies": Some institutions are listed as "investigative bodies" in the Act (for example, the RCMP and CSIS). An investigative body can ask another federal institution to provide it with personal information to assist it in carrying out its activities. However, the

[10] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182.

[11] Commission of Inquiry into the Actions of Officials in Relation to Maher Arar.

other institution must be asked first. It cannot decide on its own to proactively share personal information with an investigative body.

3. "Public interest": The head of a federal institution may disclose personal information if the head determines that the public interest benefit in disclosure clearly outweighs any invasion of privacy. In the national security context, communicating what the benefit is to a non-national security institution to obtain disclosure may not be possible (for example because of operational sensitivities). This makes it difficult for the head of the non-national security institution to decide whether to disclose personal information in the public interest.

4. "Lawful authority": the *Privacy Act* permits disclosure of personal information where another Act of Parliament authorizes it.

Consider a scenario…

A foreign national, Ms. E, sends an application for permanent resident status to Immigration, Refugees and Citizenship Canada (IRCC). This application contains the personal information that the Government needs to process her request to become a permanent resident and to determine whether she is admissible to Canada under the *Immigration and Refugee Protection Act*. To assess her application for security concerns, IRCC discloses some of Ms. E's personal information to CSIS, which has a security screening mandate under the immigration program. This type of sharing between IRCC and CSIS is an example of sharing that takes place under the "consistent use" exception of the *Privacy Act*.

The *Security of Canada Information Sharing Act*

Objective

The ATA, 2015 enacted the *Security of Canada Information Sharing Act* (SCISA) to facilitate national security information sharing. The SCISA creates an explicit disclosure authority, which provides greater certainty about when institutions can share information for national security reasons. Because it is an Act of Parliament that authorizes disclosure, it satisfies the "lawful authority" exception under the *Privacy Act*, as explained above.

What the SCISA Does

The SCISA authorizes all federal institutions to disclose information (including information about individuals) related to "activities that undermine the security of Canada." "Activity that undermines the security of Canada" is defined as any activity that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada" (section 2 of the SCISA). This concept covers a broad range of national security-related activities and is intended to provide flexibility to accommodate new forms of threats that may arise. The SCISA includes examples of these activities that may be covered by this concept.

Information may be disclosed to 17 federal institutions listed in the SCISA (referred to as "recipients" throughout this document).[12] To be disclosed, the information must be *relevant*[13] to the recipient's lawful national security jurisdiction or responsibilities.

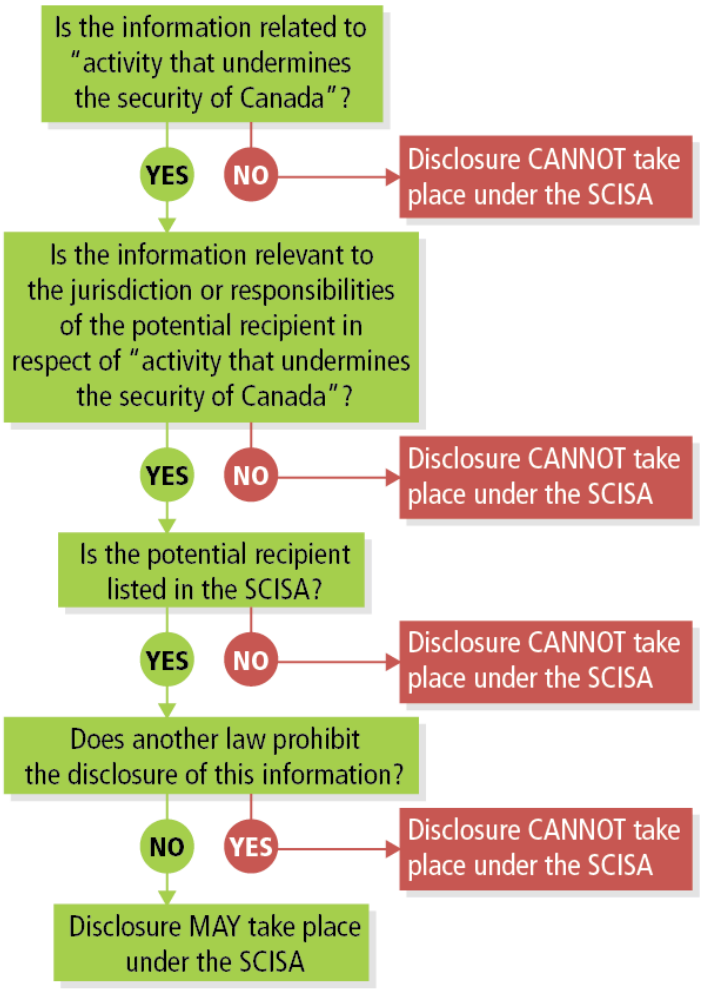
Consider a scenario…

During a routine check, a passport official at IRCC contacts the references of Mr. F, who has applied for a passport. Mr. F has been attending Mr. A's weekly meetings. Without prompting, one referee tells the passport official that she is worried that Mr. F may be travelling to a country to become a fighter with a terrorist group, since he supports the group's goals. IRCC proactively shares information under the SCISA with CSIS and the RCMP, which have responsibilities for investigating this type of activity.

To decide whether they can disclose information under the SCISA, federal institutions go through the following process:

[12] These 17 recipients already have legal authorities to collect information for national security reasons. The SCISA neither expands nor changes these collection authorities.

[13] Relevant: Because national security information sharing often engages privacy rights, the SCISA requires that information be disclosed only if it is actually—and not potentially or possibly—relevant to the recipient's lawful responsibilities for activity that undermines the security of Canada. There must be a reasonable basis to conclude that the information is related to the recipient's exercise of their responsibilities for such activity. Reliability and accuracy are also important factors in determining whether information is relevant under the SCISA.



When the SCISA Can and Cannot be Used:

The definition of "activity that undermines the security of Canada" only includes activities that have an impact on national security. Some Canadians expressed concern during the parliamentary examination of the bill that became the ATA, 2015 that their right to lawful protest may be impacted by the SCISA. The SCISA was amended to make it clear the activities of advocacy, protest, dissent, and artistic expression *do not* fall within the definition of "activity that undermines the security of Canada." As a result, information about these activities cannot be disclosed under the SCISA.

However, if violent actions take place that meet the definition of "activity that undermines the security of Canada," they cannot be considered to be advocacy, protest, dissent or artistic expression. Information about these actions can be disclosed under the SCISA.

Consider another scenario…

A national park is located near a natural gas pipeline, a critical infrastructure site. An official at the park notices a group gathering to protest near the pipeline. Even though this information deals with critical infrastructure, the official cannot disclose this information under the SCISA to another federal institution. This is because protest, advocacy, dissent, and artistic expression are explicitly excluded from the definition of "activity that undermines the security of Canada" under the SCISA.

What the SCISA Does Not Do

The SCISA cannot be used to bypass other laws prohibiting or limiting disclosure. If another law restricts use or sharing of information, these restrictions continue to apply and must be respected. For example, Employment and Social Development Canada's program legislation addresses how it protects and discloses personal information. The SCISA does not override this program legislation.

Who Decides Whether to Use the SCISA?

The institution disclosing information is responsible for determining whether the information may be disclosed. The disclosing institution may need discussions with the potential recipient to see if the information relates to the national security responsibilities of the recipient. These discussions should not require the sharing sensitive operational information.

An institution has the discretion whether or not to disclose information under the SCISA. This decision always rests with the disclosing institution even if all the SCISA requirements for disclosure are met.

Who Receives the Information?

All recipients under the SCISA have national security responsibilities. However, not necessarily all parts of the recipient institutions will be involved in carrying out these responsibilities. The SCISA requires that information be provided to the head of the institution or to delegates of the head. This helps to ensure that only officials who need the information receive it.[14]

Potential Impacts on *Charter* Rights

The *Charter* protects individuals' privacy against unreasonable government intrusions. The *Charter* allows intrusions into privacy that are authorized by a reasonable law. In some cases, disclosure of information among federal institutions could impact privacy rights.

Information sharing under the SCISA may be reviewed like other instances of government information sharing. In particular, the *Privacy Act* allows the Privacy Commissioner of Canada to review institutions' handling of personal information and to hold institutions accountable by

[14] Once information is disclosed to a recipient under the SCISA, the recipient may further disclose it under the SCISA or under another authority outside the SCISA. The recipient's use of the information disclosed to it under the SCISA continues to be governed by authorities found outside the SCISA.

releasing public reports. Some institutions – the RCMP, CSIS and the CSE – also have specific bodies that review their work, including information sharing practices that are part of this work.

The SCISA includes a power to make regulations; however no regulations have been made. Regulations made under the SCISA would support how the SCISA works in practice. For example, regulations could outline record-keeping requirements.

A number of government-wide information sharing guidance and support resources are available for federal institutions. Public Safety Canada has prepared a deskbook and a public framework to guide institutions in using the SCISA. Federal institutions may also set policies and give guidance on how their officials should use the SCISA.

What are other countries doing?

Many countries seek to promote the sharing of information for national security purposes, while protecting the privacy rights of individuals. As each country has a unique legislative and policy framework for the sharing of information for national security purposes, the challenges they face in this area vary considerably across jurisdictions. Some countries allow the sharing of information between government agencies without express consent to do so in each case. Others have more explicit powers or policies.

The UK's information sharing provisions are included in its *Counter-Terrorism Act, 2008*. These provide broad information sharing powers, including from persons to UK security agencies. Denmark has express authority in privacy legislation (the *Act on Processing of Personal Data*) to share personal information for national security purposes. Australia has a 10-year plan (Vision 2020) to enhance national security information sharing, which includes a harmonized policy and legislative framework.

What do you think?

The Government has made a commitment to ensure that Canadians are not limited from lawful protest and advocacy. The SCISA explicitly states that the activities of advocacy, protest, dissent, and artistic expression do not fall within the definition of "activity that undermines the security of Canada." Should this be further clarified?

Should the Government further clarify in the SCISA that institutions receiving information must use that information only as the lawful authorities that apply to them allow?

Do existing review mechanisms, such as the authority of the Privacy Commissioner to conduct reviews, provide sufficient accountability for the SCISA? If not, what would you propose?

To facilitate review, for example, by the Privacy Commissioner, of how SCISA is being used, should the Government introduce regulations requiring institutions to keep a record of disclosures under the SCISA?

Some individuals have questioned why some institutions are listed as potential recipients when their core duties do not relate to national security. This is because only part of their jurisdiction or

responsibilities relate to national security. Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?

THE PASSENGER PROTECT PROGRAM

Air travel is an important means of transportation, both within Canada and abroad. Without appropriate security measures, air travel is vulnerable to criminal and national security threats. Tragedies such as the 1985 Air India bombing, the attacks of September 11, 2001, and the October 2015 bombing of a Russian airliner in Egypt, each demonstrate the cost in lives, economic and social disruption that threats to aviation security can cause.

Direct threats to aviation security, such as terrorists bringing or placing explosive devices aboard aircraft, continue to be of concern. In addition, concern is growing about individuals travelling abroad, often by air, to engage in terrorism offences. These individuals are known as "extremist travellers." They pose a threat at home and also pose a threat abroad when they participate in conflicts in countries as Syria and Iraq. These individuals are involved in training, fundraising and other terrorist activities on behalf of groups such as Daesh. Trained, radicalized and experienced extremist travellers pose another serious risk if they return to Canada. Here, they might launch or inspire domestic attacks.

The Government provides aviation security in part by preventing individuals who have the intent and capability to harm passengers and aircraft from boarding. The ATA, 2015 enacted the *Secure Air Travel Act* (SATA). Under the SATA, the Government can use the Passenger Protect Program (PPP) – an air passenger identity screening program – to prevent individuals from boarding a flight if they pose a threat to transportation security or are seeking to travel by air to commit certain terrorism offences.

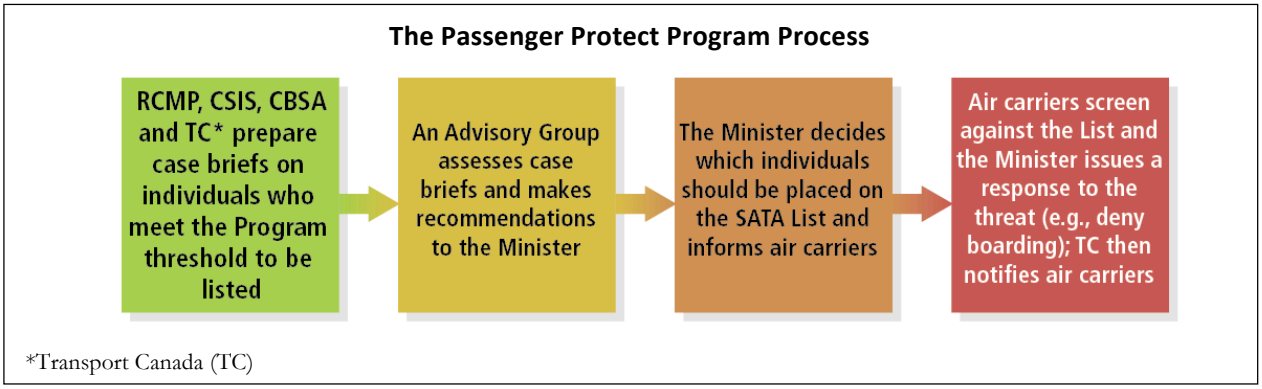
Consider a scenario…

Ms. G is a 22-year-old high school graduate who has been drifting between jobs over the past few years. She attends Mr. A's discussion meetings in her neighbourhood and has rapidly radicalized to violence.

Ms. G is keen to travel overseas to join a terrorist group. Mr. A has been communicating with a terrorist overseas to plan Ms. G's departure. The goal is for Ms. G to get weapons and explosives training and fight for her cause. She then wants to return to Canada and train others to become terrorists.

The RCMP become aware of Ms. G's plans and alert Public Safety Canada. Based on this information, the Minister of Public Safety and Emergency Preparedness adds Ms. G to the list created under the SATA. If Ms. G attempts to check in for a flight, Public Safety Canada will be alerted and may issue a direction to deny her boarding.

The PPP, as governed by the SATA, works as follows:



Through the PPP, the Minister of Public Safety and Emergency Preparedness (the Minister[15]) has the authority to establish a list of individuals (known as the SATA List) who may (1) pose a threat to transportation security or (2) travel by air to commit certain terrorism offences.[16] Listed individuals can be prevented from flying. To list an individual, the Minister must have reasonable grounds to suspect that the individual will engage in at least one of these two acts. For example, if it is reasonably suspected that an individual will travel by air to commit certain terrorism offences,[17] such as to participate in the activities of a terrorist group, the individual can be listed under the PPP.

The listing process is conducted confidentially and is based on intelligence and other information from investigations. Public Safety Canada chairs an advisory group composed of the RCMP, CSIS, the CBSA, TC and IRCC. The advisory group nominates individuals to the SATA List, assesses the information supporting the nominations and recommends to the Minister which individuals should be listed. The SATA List is reviewed at least every 90 days to ensure that there are still reasonable grounds to suspect that individuals on the List pose a threat to transportation security and/or will travel by air to commit certain terrorism offences.

Once an individual is listed, the Minister can direct an air carrier on how to respond when the individual attempts to board an aircraft. The direction will be issued to air carriers only once an individual's identity is verified and confirmed to be a positive match to the SATA List, and after any new information is considered. These responses are tailored to the specific situation, based on what is reasonable and necessary to prevent the threat from being carried out. For example, individuals who are assessed as posing a high risk to transportation security may be denied boarding to protect both passengers and aircraft. Other listed individuals may undergo additional screening to provide greater certainty that they are not, for example, carrying any weapons or prohibited items.

---

[15] The Minister can delegate his or her authority to take any action under the SATA.

[16] Pursuant to paragraphs 8(1)(*a*) and (*b*) of the SATA.

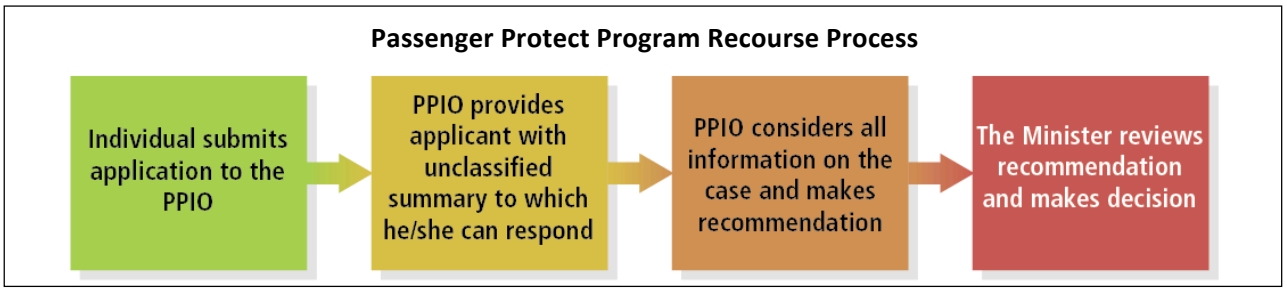
[17] The SATA refers to offences under sections 83.18, 83.19 and 83.2 of the *Criminal Code*.

Potential Impacts on *Charter* Rights

A direction to deny boarding can impact a citizen's right to enter and leave Canada. Section 6 of the *Charter* protects this right. Individuals also have an interest in not being delayed or prevented from travelling by air. A direction to deny boarding would only be made when the Minister considers it is reasonable and necessary to prevent a listed person from taking a specific action.

Recourse

Because of the acknowledged impacts of being denied boarding, an individual in this situation can apply in writing for recourse to the Passenger Protect Inquiries Office (PPIO) within 60 days of being denied boarding.[18] The application seeks to have the individual's name removed from the List. The applicant receives an unclassified summary of the information used to support the listing and has an opportunity to respond. The Minister may take up to 90 days[19] to review the application and decide whether there are still reasonable grounds to maintain the applicant on the List. If the Minister does not make a decision within 90 days,[20] the Minister is deemed to have decided not to remove the applicant's name from the List. This is done to err on the side of caution, while the 90-day deadline ensures that the applicant has timely access to the Federal Court, as explained below.



If an individual is not satisfied with the Minister's decision, the individual may appeal the decision to the Federal Court. Most decisions made under the PPP rely on sensitive information that, if disclosed, could be injurious to national security or endanger the safety of a person. The judge hearing the appeal can see all information relevant to the Government's decision. To protect against disclosure of sensitive information, the applicant sees a summary of the relevant sensitive information. The applicant can also introduce new information to respond to the Government's case. The judge may appoint an *amicus curiae* to assist the Court with any aspect of the proceeding, including during the closed portion of the proceedings where the applicant cannot be present because sensitive information is being presented.

[18] Subsection 15(2) of the SATA allows the Minister to extend that limit if there are exceptional circumstances.

[19] Subsection 15(6) of the SATA allows this period to be extended, as agreed by the applicant and the Minister.

[20] Or a further period agreed upon between the applicant and the Minister.

Consider a scenario…

Mr. H intends to fly to Florida for the Labour Day weekend but is delayed at the airline ticket counter while the desk agent contacts his supervisor. After a few minutes, Mr. H is allowed to continue, but he leaves on his flight frustrated. He suspects that his name is similar to that of someone on Canada's aviation security list. He contacts the Passenger Protect Inquiries Office, which works with relevant partners to help facilitate his future travel.

Redress

The SATA List is not the only reason for delaying an individual or preventing them from flying. There can be many other reasons, unrelated to the SATA, including air carriers' own security lists and/or aviation security lists maintained by other countries. As well, a false positive match to an aviation security list, whether that of an air carrier, a foreign country or the SATA List itself, may cause travel to be delayed.

The PPIO provides assistance to air travellers who have experienced delays or difficulties related to aviation security lists. The PPIO can assist the traveller in identifying the reason for this situation and suggest what to do next. Following a joint announcement by the Prime Minister of Canada and the President of the United States on March 10, 2016, the governments established the Canada-U.S. Redress Working Group. The Working Group is a bilateral mechanism. It allows the PPIO to collaborate closely with the U.S. on certain matters of redress and recourse about Canadian and American citizens and permanent residents who may be affected because of their potential presence on the SATA List or the U.S. No Fly List.

In addition, the Government is considering possible changes to the SATA and its regulations to help reduce instances of false positive matches to the SATA List. The objective is to create a process where individuals who have experienced a false positive match can obtain a redress number, which would be provided to the air carrier prior to travel and assist in avoiding delays.

What are other countries doing?

A number of Canada's key international partners, including the U.S., the UK, Australia and New Zealand have some form of air passenger screening prior to departure. In most cases, these programs are designed to determine an individual's admissibility status before they can travel to that country, and/or whether they pose a security risk. The U.S., for example, operates a number of air passenger screening programs that address both immigration and security considerations.

Canada's PPP does not operate in conjunction with the U.S. No Fly list or with any other countries' and organizations' aviation security programs. While the SATA permits the Minister of Public Safety to share information with another country to address potential threats, both countries' programs will continue to operate subject to their respective laws.

What do you think?

At present, if the Minister does not make a decision within 90 days about an individual's application for removal from the SATA List, the individual's name remains on the List. Should this be changed, so that if the Minister does not decide within 90 days, the individual's name would be removed from the List?

To reduce false positive matches to the SATA List, and air travel delays and denials that may follow, the Government has made a commitment to enhance the redress process related to the PPP. How might the Government help resolve problems faced by air travellers whose names nonetheless generate a false positive?

Are there any additional measures that could enhance procedural fairness in appeals of listing decisions after an individual has been denied boarding?

CRIMINAL CODE TERRORISM MEASURES

The *Criminal Code* defines terms such as "terrorist activity," "terrorism offence" and "terrorist group." It sets out a wide range of terrorism offences, provides a process to "list" entities as terrorist groups and outlines a range of anti-terrorism powers for law enforcement.[21] Many of the terrorism provisions were enacted in 2001 and amended in 2013 to include specific terrorist travel offences. Since 2001, a number of people have been convicted of terrorism offences in Canada, with some receiving life sentences. The courts have found key *Criminal Code* terrorism provisions to be consistent with the *Charter*.[22]

Some provisions of the ATA, 2015 introduced changes to *Criminal Code* terrorism provisions. The Code was amended to accomplish several goals:

- to make it easier for peace officers to detain individuals temporarily, and to apply to a court to have reasonable conditions imposed on individuals to prevent the carrying out of terrorist activity and the commission of terrorism offences;
- to create a new offence that criminalizes the advocacy or promotion of the commission of terrorism offences in general;
- to give the courts the authority to order the seizure and forfeiture of tangible terrorist propaganda material and the removal of online terrorist propaganda from Canadian websites; and,
- to provide additional protection to witnesses and other participants in national security proceedings and prosecutions.

Preventive Law Enforcement Tools (Recognizance with Conditions and Terrorism Peace Bond)

Canadian criminal law generally focuses on prosecuting offences that have already occurred. However, criminal courts can also impose **preventive conditions** on an individual where there is evidence that the individual is likely to commit an offence in future. Two specific tools allow for a court to impose conditions to prevent terrorism: the **recognizance with conditions** and the **terrorism peace bond**. Some aspects of these tools first appeared in 2001 when the *Anti-terrorism Act* came into force.

---

[21] "Terrorist activity" is a term made up of a list of specific offences that implement Canada's international obligations, as well as a general definition. It is used as the basis for many of the terrorism offences in the *Criminal Code*, such as knowingly facilitating a terrorist activity

[22] See, for example, *R. v. Khawaja* [2012] 3 SCR 555.

A **terrorism peace bond** is used to prevent a specific individual from committing a terrorism offence, such as leaving or attempting to leave Canada to commit an offence for a terrorist group.

A **recognizance with conditions** is used when the police suspect someone is connected in some way to the carrying out of a terrorist activity. For example, they suspect that someone is connected to a broad plot to attack Parliament, but the person's exact role may not be known.

Both the terrorism peace bond and the recognizance with conditions aim to prevent individuals from carrying out terrorist acts.

Consider a scenario where a terrorism peace bond could be used…

A family notifies the RCMP that they feel their son, Mr. I, has become radicalized to violence. He is a good friend of Mr. A. The RCMP investigate and learn that Mr. I has told a number of people close to him that he plans to join a terrorist group active in a conflict zone abroad. The RCMP also learn that Mr. I has been pricing air travel to a country that borders an ongoing conflict zone where the group is active.

The RCMP now suspect that Mr. I may commit a terrorism offence – travelling or attempting to travel abroad to participate in the activity of a terrorist group. They seek the consent of the Attorney General of Canada to apply to a judge for a terrorism peace bond to prevent Mr. I from travelling abroad.

Consider a scenario where a recognizance with conditions could be used…

The police conduct an urgent investigation into a group of ten people based on an anonymous tip. Some of these people attend Mr. A's weekly meetings. Some members of the group are apparently planning to bomb an unknown public gathering that week. Further investigation reveals that one person in the group, Ms. J, recently downloaded bomb-making instructions. The police hope to obtain a recognizance with conditions to stop Ms. J from making, providing or using an explosive device. They seek the consent of the Attorney General of Canada to apply to a judge for a recognizance with conditions.

The judge considers the application and is satisfied that a terrorist activity may be carried out. The judge also has reasonable grounds to suspect that the imposition of the recognizance with conditions is likely to prevent the carrying out of the terrorist activity. As a result, the judge issues a recognizance with conditions.

The ATA, 2015 amended the provisions on recognizance with conditions and the terrorism peace bond. The amendments were designed to make it easier for police to apply to provincial court for the imposition of reasonable conditions, such as travel restrictions.

The 2015 amendments did the following:

- lowered the threshold to obtain a **recognizance with conditions** to where a peace officer believes on reasonable grounds that a terrorist activity "may be carried out." Previously, the law required that police believe on reasonable grounds that a terrorist activity "will be carried out." The amendments also replaced the former requirement that a recognizance is "necessary to prevent" the carrying out of a terrorist activity with "is likely to prevent."

- increased the period of detention before a recognizance with conditions hearing is held to up to seven days, which includes periodic review by a judge. Previously, such detention could last only up to three days – a possible 24-hour police-initiated detention and a 48-hour judge-ordered detention.

  Further periods of detention beyond the possible 24-hour initial police detention are allowed only if the judge finds that it is necessary to ensure public safety, to ensure that the person attends the hearing or to maintain confidence in the administration of justice. In addition, there are two new possible 48-hour periods of judge-ordered detention. In these instances, it must also be demonstrated that the investigation in relation to which the person is being detained is being conducted "diligently and expeditiously." If these criteria are not met, the person must be released – with or without conditions – but will be required to return to court for the hearing on whether conditions should be imposed on them.

- lowered the threshold to obtain a **terrorism peace bond** so that it may be obtained when a person believes an individual "may commit" a terrorism offence. Previously, the threshold was "will commit" a terrorism offence.

- for both the recognizance with conditions and the terrorism peace bond, there are now additional requirements for the judge to consider whether to impose a geographical restrictions condition on the person and whether to require the person to surrender their passport(s) or other travel documents.

- increased the length of time these measures can be applied if the person has been previously convicted of a terrorism offence. For the recognizance with conditions, the conditions can apply for up to two years. For the terrorism peace bond, the conditions can apply for up to five years.

- if a person breached their conditions under a recognizance with conditions or a terrorism peace bond, increased the maximum penalty to four years imprisonment (from a maximum of two years).

- sought to improve the efficiency and effectiveness of the recognizance with conditions and peace bonds across Canada by allowing for the use of video conferencing and for the transfer of peace bonds between provinces.

Potential Impacts on Charter Rights

The terrorism peace bonds and recognizance with conditions impact liberty interests protected under the *Charter*. Persons subject to these measures may face detention and other restrictions on their liberty without being charged with or convicted of an offence.

The consent of the Attorney General of Canada or of a province is required before the police can even apply to a judge for a recognizance with conditions or terrorism peace bond. In addition, the Crown or the affected person may apply to change any of the conditions. The recognizance with conditions also continues to be subject to a requirement to report annually on its use, whereas no similar reporting requirement applies in respect of the terrorism peace bond. Finally, the provisions on these recognizances are subject to a five-year sunset clause. This means that the recognizance provisions will no longer be in force five years after July 15, 2013, unless Parliament renews them.

Criminalizing the Advocacy or Promotion of Terrorism Offences in General

The ATA, 2015 added a new *Criminal Code* offence on advocating or promoting the commission of terrorism offences in general.

Consider a scenario…

Ms. K has also been attending Mr. A's weekly discussion groups. She feels that what Mr. A is saying should be known by more people and that Mr. A's views deserve a wider audience. To do this, Ms. K has started posting some of her views online. Over time, she has gained some followers on social media. She is now clearly stating that violence should be used as the only way to change the Government's position on foreign policy.

Ms. K has been communicating with some of her online followers. One has stated that they would be willing to "take direct action." In response to what she believes is support for her views, she decides to use her latest post to appear in a video message dressed in military clothing. In the video, she urges her followers to support a terrorist group by saying, "Do not wait for us to tell you what to do. From now on, you have permission to do whatever you want, do whatever is in your capability. Just act."

As noted above, the 2015 change to the *Criminal Code* makes it a criminal offence for a person, by communicating statements, to knowingly advocate or promote the commission of terrorism offences in general. To commit the offence, the person must *know* that any of those offences will be committed or *be reckless* as to whether any of those offences may be committed as a result of such communication.

Counselling generally involves one person procuring, soliciting or inciting another to commit a criminal offence. Counselling is a long-standing offence. It requires some specificity about the offence or type of offence being counselled.

The definition of "terrorism offence" in the *Criminal Code* includes a broad range of conduct – from violence against people and destruction of property to providing financial and material support and recruitment. Before the 2015 change to the *Criminal Code*, the scope of the offence of counselling was unclear. There was some uncertainty about whether it constituted counselling if a person actively encouraged committing terrorism offences but was not specific about the offences or the type of offences (for example, whether terrorist bombing or terrorist financing). There was also uncertainty about what the penalty would be. This new offence makes it clear that such conduct is criminal. The new offence is modelled on the existing law of counselling. It extends the concept of counselling to cases where no specific terrorism offence is being counselled, but where it is evident nonetheless that terrorism offences are being counselled.

The maximum penalty for the new offence is five years imprisonment. This is the same maximum as that for advocating or promoting genocide against an identifiable group, the most serious of the three hate propaganda offences in the *Criminal Code*.

Potential Impacts on Charter Rights

Because this offence criminalizes communicating statements, it could be viewed as limiting freedom of expression. However, it is important to consider that the expression in question is generally directed at violent activities. As well, this offence involves more than mere expression. The offence is not an attempt to criminalize glorification of terrorism or praise of terrorism. The offence prohibits active encouragement to commit terrorism offences, not mere expressions of opinion about the acceptability of terrorism.

To ensure appropriate oversight, the prior consent of the appropriate Attorney General is needed to begin proceedings in respect of terrorism offences.

Seizure and Forfeiture (or Removal) of Terrorist Propaganda

The ATA, 2015 created two new warrants of seizure (court orders that allow police to seize materials) in the *Criminal Code* to apply to "terrorist propaganda" material. This is material counselling the commission of a terrorism offence or advocating or promoting the commission of terrorism offences in general.

Related amendments to the *Customs Tariff* also allow CBSA border services officers to seize terrorist propaganda being imported into Canada without a warrant, as they would other contraband.

Some Canadians raised concerns about the definition of terrorist propaganda during the debate about the ATA, 2015. The Government has made a commitment to address the issue.

The new provisions allow a judge to order the seizure and forfeiture of terrorist propaganda material that is in printed form or is in the form of audio recordings. A judge may also order the removal of terrorist propaganda when it is in electronic form and is made available to the public through a Canadian Internet service provider (ISP).

Continuing the scenario from above…

Ms. K's posts on social media are made available through a Canadian ISP. Her posts have clearly been promoting the commission of terrorism offences in general.

With the consent of the Attorney General, the police seek a warrant from a judge requiring the Canadian ISP to remove this content from the site.

Potential Impacts on Charter Rights

The new warrants could impact the right to free expression. However, the warrants are similar to those already available under the *Criminal Code* for the seizure of material deemed criminal, such as hate propaganda. As well, the consent of the Attorney General is needed before the police can apply for a warrant, to ensure that the Attorney General considers public interest issues, such as protecting freedom of expression.

Protections for Witnesses and Other Justice System Participants

The ATA, 2015 introduced changes to the *Criminal Code* to improve protection of witnesses, in particular in proceedings involving security information or criminal intelligence information. Security certificate proceedings under the *Immigration and Refugee Protection Act* are examples.

The changes on how witnesses can testify include the following:

- Judges can order that witnesses testify behind a device, such as a screen, to prevent the public from seeing them while they testify;
- Judges must consider whether a witness has responsibilities relating to national security or criminal intelligence when deciding whether to allow that witness to testify using a pseudonym or via closed-circuit television; and
- Judges have explicit authority to make any order necessary to protect the security of any witness, including those who have responsibilities relating to national security. One such order could be to allow a witness to testify while partially disguised.

In addition, the ATA, 2015 amended the *Criminal Code* to better protect justice system participants from intimidation. The *Criminal Code* prohibits their intimidation and provides a maximum of 14 years imprisonment for the offence. The ATA, 2015 amended the *Criminal Code* to expand the definition of "justice system participant" to include persons who play a role in proceedings that involve various types of information, including security information and criminal intelligence information. This ensures that punishment for intimidation is proportional to the gravity of the conduct, its effect on the victims and, more broadly, its effect on the proper functioning of the justice system.

The ATA, 2015 also amended the *Criminal Code* to remove the requirement to publish the names of federally-designated prosecutors and peace officers who have obtained authorizations to intercept private communications ("wiretap" authorizations). This increases protection from intimidation or retaliation for federal prosecutors and law enforcement officers who obtain such authorizations. The amendment puts them in the same situation as their provincial counterparts. The Minister of Public Safety and Emergency Preparedness will continue to report annually to Parliament on the number of federally-designated prosecutors and peace officers who have obtained authorizations for wiretaps. This maintains ministerial accountability for their use.

Potential Impacts on Charter Rights

These measures on how witnesses can testify could impact the open court principle (the principle that information before a court ought to be public information as far as is possible), which is protected by the *Charter*, because the public is deprived of some information about the proceeding.

These measures could also impact fair trial rights because some witnesses may testify behind a device shielding their identity.

What are other countries doing?

Terrorism Peace Bonds and Recognizance with Conditions

The recognizance with conditions and peace bond provisions are consistent with counter-terrorism laws in countries such as the UK and Australia.

The UK, for example, currently allows for pre-charge detention in respect of a terrorist offence for up to 14 days, which also requires independent review on grounds similar to those contained in the ATA, 2015. They also have a tool similar to a peace bond, called a Terrorism Prevention and Investigation Measure, which allows for the imposition of conditions on individuals where satisfied, on the balance of probabilities, that the individual is or has been involved in terrorism-related activity.

Australia also allows for preventative detention which, under federal law, can last for three days. Australian law also permits the imposition of "Control Orders," which are similar to peace bonds and which can result in the imposition of conditions on individuals where evidence establishes that, for example, making the order would substantially assist in preventing a terrorist act.

Advocacy or Promotion of Terrorism Offences in General

Since 2006, the UK has had an offence of direct or indirect encouragement to commit acts of terrorism. For the purposes of the offence, it is irrelevant whether the encouragement relates to one or more particular acts of terrorism or acts of terrorism generally. Indirect encouragement is defined to include a statement which glorifies the commission of such acts and which members of the public could reasonably be expected to infer that what is being glorified is being glorified as conduct that should be emulated by them in existing circumstances.

In 2014, Australia created a new offence of advocating the doing of a terrorist act or the commission of a terrorism offence, while being reckless as to whether another person will engage in a terrorist act or commit a terrorism offence. "Advocates" is defined to include promoting. It applies where one terrorism act or offence is being advocated or more than one of such acts or offences are being advocated. There are statutory defences that may apply depending on the circumstances, such as publishing in good faith a report or commentary about a matter of public interest. The maximum punishment is five years imprisonment.

As the Canadian offence in ATA, 2015 is based on the knowing and active encouragement of the commission of terrorism offences in general, it more closely resembles the Australian rather than the UK model.

Seizing Terrorist Propaganda

The measures are similar to laws that already exist in the UK and Australia. For example, the UK legislation, which allows for the takedown of websites and social media feeds, has been in existence since 2006. In Australia, complaints about on-line content are made to the Australian Communications and Media Authority (ACMA). If the ACMA determines that the content is restricted (i.e., if it incites violence or advocates a terrorist act), it issues a notice and takedown order to the service provider.

Protecting those Involved in National Security Proceedings/Prosecutions

The UK, New Zealand, and Australia have all developed legislative regimes that provide ways for witnesses to testify which seek to mitigate any adverse consequences that may arise from their giving testimony, while protecting the interests of an accused.

What do you think?

Are the thresholds for obtaining the recognizance with conditions and terrorism peace bond appropriate?

Advocating and promoting the commission of terrorism offences in general is a variation of the existing offence of counselling. Would it be useful to clarify the advocacy offence so that it more clearly resembles counselling?

Should the part of the definition of terrorist propaganda referring to the advocacy or promotion of terrorism offences in general be removed from the definition?

What other changes, if any, should be made to the protections that witnesses and other participants in the justice system received under the ATA, 2015?

PROCEDURES FOR LISTING TERRORIST ENTITIES

Listing an individual or group as a "terrorist entity" is a public means of identifying their involvement with terrorism and curtailing support for them. Listing is one component of the international and domestic response to terrorism.

There are three listing mechanisms in Canada. Two are established under Canada's *United Nations Act*[23] and a third was created by an amendment to the *Criminal Code* in 2001. Domestically, Canada relies mainly on the *Criminal Code* process. The *Criminal Code* process both helps to fulfill Canada's international obligations and supports domestic counter-terrorism measures. An entity listed under the *Criminal Code* fall under the *Criminal Code*'s definition of a terrorist group. Any funds the group has in Canada are immediately frozen and may be seized by, and forfeited to, government.

More than 50 terrorist entities are now listed under the *Criminal Code*. These include al-Qaida and Daesh. To date, most listed entities are based overseas, though members or supporters can also be found in Canada. Entities originating in Canada can also be listed.

The *Criminal Code* listing process begins with the RCMP or CSIS producing criminal or security intelligence reports on an entity. The Minister of Public Safety and Emergency Preparedness may recommend to the federal Cabinet that an entity be listed if the Minister has reasonable grounds to believe that the entity:

- knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity; or
- is knowingly acting on behalf of, at the direction of, or in association with an entity that has knowingly carried out, attempted to carry out, participated in or facilitated a terrorist activity.

To list an entity, Cabinet must also be satisfied that the above test is met. The name of the listed entity is then published in the *Canada Gazette*. A complete list is available on Public Safety Canada's website.

Consider a scenario…

The 123 Group has committed terrorist attacks overseas and is being investigated by CSIS. CSIS informs Public Safety Canada about 123 Group's involvement in these attacks and its links to Canada. The Minister of Public Safety and Emergency Preparedness recommends to Cabinet adding the 123 Group to the list of terrorist entities established under the *Criminal Code* because the group has knowingly carried out a terrorist activity. Cabinet approves the listing. All financial assets

[23] These are the *UN Al-Qaida and Taliban Regulations* and the *Regulations Implementing the UN Resolutions on the Suppression of Terrorism*.

belonging to 123 Group in Canada are frozen and can be seized by government.

The entity and the public are not made aware that the Government is planning to list the entity until the listing takes effect. This is to prevent the entity removing its Canadian assets from Canada before the listing freezes them.

Once an entity is listed, the *Criminal Code* deems it a "terrorist group" in Canada. This can help with investigating and prosecuting terrorism offences since it is not necessary for investigators and prosecutors to prove independently that the individual or group is a terrorist group. It is not a crime simply to be a terrorist group, but many *Criminal Code* terrorism offences contain the term "terrorist group" in the description of the offence. For example, it is an offence to do any of the following:

- knowingly participate in, or contribute to any activity of, a terrorist group for the purpose of enhancing the ability of any terrorist group to facilitate or carry out terrorist activity;
- leave Canada to participate in the activities of a terrorist group;
- collect money or property knowing that it will benefit a terrorist group; and,
- instruct anyone to carry out an activity for the benefit of a terrorist group.

The listing process also makes it easier to apply other provisions relating to terrorist groups, such as using the *Charities Registration (Security Information) Act* to de-register a charity or refuse to register an organization as a charity.

Canada's closest allies, including the U.S., UK, Australia and New Zealand, have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations.

Potential Impacts on *Charter* Rights

Being listed as a terrorist entity or being associated with a terrorist entity could impact *Charter* rights. Specifically, section 7 of the *Charter* protects against the deprivation of life, liberty and security of the person, except in accordance with the principles of fundamental justice.

Procedural safeguards have been put in place because of the possible impact of a *Criminal Code* listing on these rights. An entity has the right to apply to the Minister of Public Safety and Emergency Preparedness to be de-listed. If the Minister decides not to de-list the entity, the entity can ask the Federal Court for judicial review of the Minister's decision.

Some of the evidence relating to the listing will be sensitive, and the Government may wish to protect it from being disclosed to the entity. However, this evidence can only be withheld from the entity if a Federal Court judge determines that its disclosure would injure national security or endanger the safety of any person. If evidence is withheld on these grounds, the judge must provide

an unclassified summary to ensure that the entity can understand the basis of the listing decision. As part of this process, the entity can also make submissions to the Federal Court. If the judge determines that the listing is unreasonable, he or she will order the entity to be de-listed.

The Government is also required to review all entities on the list every two years and confirm whether they should remain on the list.

Listing an entity could harm individuals and groups with a similar name. To prevent harm from mistaken identity, individuals and groups may apply to the Minister of Public Safety and Emergency Preparedness for a certificate confirming that they are not the entity on the list.

What are other countries doing?

Canada's closest allies all have similar terrorist listing regimes that include mechanisms for freezing assets in compliance with international obligations. UN Security Council (UNSC) Resolution 1267 and its successor Resolutions, including UNSC Resolution 2253, require states to freeze the assets of the Taliban, Usama bin Laden and his associates, members of Al-Qaida, and members of Daesh. The Resolution also imposes a travel ban and arms embargo against those listed by the UN. Canada implements UNSC Resolution 1267 through the *UN Al-Qaida and Taliban Regulations* and through the *Immigration and Refugee Protection Act*. UNSC Resolution 1373 requires states to freeze without delay, the financial assets of persons and entities engaged in terrorism. This obligation is primarily met in Canada by the list under the *Criminal Code*, but is also implemented through the *Regulations Implementing the UN Resolution on the Suppression of Terrorism*. The manner in which these international obligations are domestically implemented by Canada's allies has led to a variety of different terrorist listing regimes.

The UK, for example, implements its international obligations in relation to UNSC Resolution 1267 using regulations made pursuant to the *European Communities Act 1972*. UNSC Resolution 1373 is implemented under Part 1 of the *Terrorist Asset-Freezing etc. Act 2010*. As well, under the UK's *Terrorism Act 2000*, the Home Secretary may proscribe an organization if it commits or participates in acts of terrorism, prepares for terrorism, promotes or encourages terrorism or is otherwise concerned with terrorism. Membership in a proscribed organization is a criminal offence. Proscribed entities may apply to the Home Office to be de-listed and, if denied, an appeal process to a special commission, as well as judicial review of its decision, is available.

Australia, like Canada, has a listing process in its *Criminal Code*. The government may list an entity if the Attorney-General is satisfied on reasonable grounds that it is directly or indirectly engaged in preparing, planning, assisting or fostering the doing of a terrorist act, or advocates the doing of a terrorist act. The Australian government reviews listed entities every three years from the date that they were originally listed. Any person or organisation is entitled to make a de-listing application to the Attorney-General and judicial review of the legality of a decision to list an organisation is also available in the courts. Australia also implements UNSC Resolution 1373 by regulations made under

the *Charter of the United Nations Act 1945,* and implements UNSC Resolution 1267 by automatically incorporating the United Nations sanctions list by regulations made under the same Act.

New Zealand's *Terrorism Suppression Act 2002* provides for a list of terrorist entities to be established and maintained. The police are responsible for coordinating requests to the Prime Minister for designation of a terrorist entity. A designation in New Zealand, like in Canada, has the effect of freezing the entity's assets. It is also a criminal offence to participate in or support the activities of the designated terrorist entity. This includes dealing with the property of the designated terrorist entity or making property or financial services available to the entity. Also, New Zealand implements the UNSC Resolution 1267 and automatically incorporates the United Nations sanctions list by regulations made under their *United Nations Act 1946*.

The lists kept by the U.S. government are more complex and diverse. The U.S. implements its obligations relating to financial sanctions under both UNSCR 1267 and UNSCR 1373 primarily through Executive Order (E.O.) 13224. The Office of Foreign Assets Control administers and enforces E.O. 13224 and maintains a public list of groups and individuals designated under the Order as well as those designated under the *Immigration and Nationality Act* as Foreign Terrorist Organizations. There are some general similarities with Canada's listing processes. For example, entities are not informed that they may be listed and they cannot provide evidence or submissions before the listing process is completed.

What do you think?

The Government is interested in your views about the listing of terrorist entities.

Does listing meet our domestic needs and international obligations?

The *Criminal Code* allows the Government to list groups and individuals in Canada and abroad. Most listed entities are groups based overseas. On which types of individuals and groups should Canada focus its listing efforts in the future?

What could be done to improve the efficiency of the listing processes and how can listing be used more effectively to reduce terrorism?

Do current safeguards provide an appropriate balance to adequately protect the rights of Canadians? If not, what should be done?

TERRORIST FINANCING

Canada has a stable, open economy, an accessible and advanced financial system, and strong democratic institutions. However, those seeking to raise, transfer and use funds for terrorism purposes try to do so by exploiting some of these strengths. In confronting the evolving challenges of terrorist financing, the Government must ensure that it does not compromise fundamental Canadian values.

Terrorist financing is a multi-faceted global phenomenon. Terrorists (individuals and groups) raise, collect and transfer funds across the globe to carry out attacks and finance day-to-day operations. They raise funds from criminal activities and from legitimate sources, such as donations or business profits. Terrorists use a variety of methods to move their funds. These include the formal banking system, international trade, money services businesses, informal money transfer systems, digital platforms, and the physical transportation of cash or certain high value goods, such as gold or precious stones.

Individuals also finance terrorist activities by raising money themselves to travel abroad for terrorist purposes or to purchase materials for attacks. Since funds are vital to terrorist organizations, depriving them of these funds is one effective mechanism to counter terrorism.

For example, one of the five priorities of the Global Coalition against ISIL is to reduce Daesh's capabilities by cutting off its access to funding. Daesh is likely the wealthiest terrorist group in the world, due to its access to proceeds generated in the territory it controls. Its wealth allows it to carry out attacks, recruit and pay members, provide training and indoctrination, maintain communications networks and disseminate propaganda. Reducing access to funds will diminish Daesh's capability.

Canada's Approach to Counter Terrorist Financing

In Canada, the Anti-Money Laundering and Anti-Terrorist Financing (AML/ATF) regime involves 11 federal departments and agencies.[24] Together, they work to prevent, detect, deter, investigate and prosecute the financing of terrorist activities. A key component of Canada's regime is the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA), which establishes FINTRAC.

The PCMLTFA imposes obligations on more than 31,000 financial service providers and financial intermediaries. The Act makes them active partners in the fight against money laundering and terrorist financing. Under the Act, these entities must keep certain records, know their customers, and report certain transactions to FINTRAC.[25] FINTRAC assesses entities' compliance with these

[24] Department of Finance, FINTRAC, the RCMP, the CBSA, CSIS, the Canada Revenue Agency, Department of Justice Canada, Public Prosecution Service of Canada, Public Safety Canada, Office of the Superintendent of Financial Institutions, and Global Affairs Canada.
[25] International electronic fund transfers (EFTs), cash transactions, disbursement from casinos over $10,000; transactions suspected of being related to ML or TF; and terrorist property reports must be reported to FINTRAC.

requirements and can fine them for non-compliance. FINTRAC also has the authority to analyze financial transaction reports and to disclose certain information to law enforcement and intelligence agencies if it has reasonable grounds to suspect that it would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence.

Law enforcement and intelligence agencies use this information and that from other sources to identify and disrupt terrorist activities. Law enforcement agencies can also lay criminal charges. The *Criminal Code* contains three terrorist financing offences. These prohibit (1) providing or collecting property for terrorist-related activities; (2) providing or making available property or services for terrorist purposes; and (3) using or possessing property for terrorist purposes. As noted earlier,[26] the *Criminal Code* also provides for a process to list individuals or groups as terrorist entities. The listing of a terrorist entity results in its property being frozen immediately. The property may then be seized and forfeited to the Government.

Consider a scenario…

Ms. L is a friend of Mr. A. She supports the 123 Group and wants to send it money abroad. Ms. L goes to a bank to send a wire transfer of $11,000 to a country where it is known that 123 Group operates. Because the amount is more than $10,000, the PCMLTFA requires the bank to report the transaction to FINTRAC. FINTRAC concludes that the transaction is suspicious (given its destination and other indicators) and provides the information to RCMP investigators.

Canada's Contribution to International Efforts

Terrorist financing is a global problem that requires a well-coordinated, multilateral response. The Financial Action Task Force (FATF), of which Canada is an active member, is an international organization that sets standards for combating money laundering and terrorist financing, which ensures all members' AML/ATF regimes are held to the same criteria. The FATF monitors the implementation of these standards among its own 37 members and the more than 190 countries in the global network of FATF-Style Regional Bodies through peer reviews and public reporting. The FATF is currently evaluating Canada against these standards and is expected to finalize and publish the results in summer 2016.

As well, Canada works with international partners through fora such as the United Nations, the G7/G20 and the Counter-ISIL Finance Group. Canada also implements several UNSC Resolutions to freeze and seize the assets of persons and entities engaged in terrorism. In addition, Canada supports regions where there is a higher risk for terrorist financing, such as the Middle East and North Africa. Canada does this through technical assistance on counter-terrorist financing. This

[26] See chapter "Terrorist Entity Listing Procedures"

assistance is designed to strengthen the capacity of financial systems in these regions to prevent them from being exploited as vehicles for terrorist financing.

Potential Impacts on *Charter* Rights

The current approach requires certain businesses to disclose private financial information to FINTRAC. FINTRAC may disclose it to law enforcement and intelligence agencies for investigation. This could impact privacy rights protected by section 8 of the *Charter*.

Because of the potential impact on section 8 privacy rights, the PCMLTFA has safeguards in place. For example, the Act prescribes the information that FINTRAC can receive and disclose. The PCMLTFA also identifies the law enforcement and intelligence agencies that can receive FINTRAC's financial intelligence. The Act also limits when FINTRAC can disclose information to these agencies. It must have reasonable grounds to suspect that the information would be relevant to the investigation or prosecution of a money laundering or a terrorist financing offence, or relevant to the investigation of threats to the security of Canada. FINTRAC is independent from law enforcement agencies and does not conduct investigations.

To ensure that the terrorist financing regime addresses emerging risks and maintains appropriate safeguards, Parliament reviews the PCMLTFA every five years. As well, the PCMLTFA requires the Privacy Commissioner of Canada to conduct a review of the measures taken by FINTRAC to protect information it receives or collects under the Act every two years. This is to ensure that FINTRAC protects the information it receives as part of its operations. The Privacy Commissioner reports the findings of the review to Parliament.

Finally, the Government continues to monitor its AML/ATF regime to ensure that it aligns with international standards and that it takes into consideration government policy priorities, including its impact on businesses and the rights of individuals.

Challenges

Canada's financial sector has evolved significantly since the PCMLFTA came into force in 2001. The Act has been amended several times in the past fifteen years, but staying current in the changing financial environment presents challenges. Financial technology is changing rapidly. The regime needs to keep pace with evolving techniques of using new platforms for illicit fundraising or financial transfers. In addition, the reporting thresholds under the Act may be set too high in terrorism matters. Banks and other financial institutions do not need to report to FINTRAC any transactions below these thresholds unless they deem them suspicious. For example, the $10,000 threshold for reporting international funds transfers may be appropriate for investigations involving money laundering, but terrorists often transfer much smaller amounts. Enhanced coverage of new technologies and a lower reporting threshold would provide more information for investigations.

However, it would also increase the personal information collected by FINTRAC, and the number of businesses required to report.

Consider a scenario…

Ms. L sends $3,000 to a member of the 123 Group outside Canada. As the transaction is below the $10,000 threshold, it is not reported to FINTRAC. The business transferring the funds has no information causing it to consider the transaction suspicious and so does not notify FINTRAC of the transaction. FINTRAC has no information to pass on to law enforcement agencies through legislated reporting mechanisms. Had FINTRAC known about the transfer, the PCMLTFA would have allowed it to inform law enforcement if it had reasonable suspicion that the transaction was related to the financing of a terrorist activity.

Terrorists are adaptable and may exploit weaknesses to avoid detection, impeding Canada's efforts to reduce terrorist financing. In addition, terrorists can procure goods or services without actual transfers of funds, limiting detection through the financial system. Terrorists have also used financial professionals with no ties with or sympathies for the terrorists' cause to help move money and resources between countries.

Terrorist financing investigations require extensive resources and significant sharing of information within Canada and with other countries. Investigation and detection also require cooperation within the private sector and between the private and the public sectors. Effective partnerships require a clear understanding by both the public and private sectors of terrorist financing methods and trends, to better and more accurately identify suspicious behaviour. These challenges suggest that an approach that adapts to technological advances and strengthens partnerships between government and the private sector, may be the most effective way to deny terrorists the resources they need.

What do you think?

The Government would like your views about how best to address gaps and other challenges in the regime.

What additional measures could the Government undertake with the private sector and international partners to address terrorist financing?

What measures might strengthen cooperation between the Government and the private sector?

Are the safeguards in the regime sufficient to protect individual rights and the interests of Canadian businesses?

What changes could make counter-terrorist financing measures more effective, yet ensure respect for individual rights and minimize the impact on Canadian businesses?

INVESTIGATIVE CAPABILITIES IN A DIGITAL WORLD

Evolving technology has changed the way Canadians communicate and live their lives. Canadians are increasingly active online. They may use multiple communications devices and a wide variety of tools such as email, Internet banking, instant messaging and various social media applications. This evolution provides enormous benefits for Canadian society, but criminals and terrorists can use these same technologies. Digital communications are now a fundamental tool for terrorism-related activities, including radicalization to violence, facilitation of travel for terrorist purposes, acquisition of funding and equipment, and even training for terrorist actions. The potential harm resulting from the exploitation of evolving technologies is not limited to national security. Traditional criminal activity – from planning violent crime to committing frauds – also relies on these technologies. New public safety challenges continue to appear via the Internet, such as the distribution of terrorist propaganda and child pornography, cyberbullying, and the "Dark Web" and its associated criminal marketplace.

Digital information is sometimes more important than physical evidence or intelligence in investigating national security threats, solving crimes and prosecuting offenders.

To protect Canadians from crime or threats to safety and security, Canada's law enforcement and national security investigators must be able to work as effectively in the digital world as they do in the physical. Law enforcement must also have the ability to cooperate effectively with their international partners who seek digital evidence from Canada to further their criminal investigations and prosecutions. The laws governing the collection of information and evidence have not, however, kept pace with the rapid advancements of digital technology in the last 20 years and the role technology plays in the lives of Canadians today. Whether information comes from more traditional sources or from within the increasingly complex digital landscape, investigators need access to that information to investigate threats to national security and criminal activity, and to cooperate with foreign partners in a timely manner.

The term "lawful access" has been used as an umbrella term to refer to certain legally authorized procedural powers and techniques, as well as criminal laws, which may come into play when national security and law enforcement agencies conduct investigations. The Government has attempted to ensure that investigative tools are adequate to deal with new forms and uses of technology. These efforts have included multiple public consultations on "lawful access"[27] and updating cybercrime

[27] These include the 2002-2003 Lawful Access Consultations, details of which can be found at www.justice.gc.ca/eng/cons/la-al/index.html.

and cyberbullying laws through the *Protecting Canadians from Online Crime Act*.[28] Canada's digital environment, however, continues to change dramatically. More data has been created in the last five years than ever before. As we move forward, discussions of the investigative capabilities of law enforcement and national security agencies in a digital world must take into account technological advances, the legal context and the current threat environment.

Potential Impacts on *Charter* Rights

Access by national security and law enforcement agencies to digital communications, information for investigative or intelligence purposes, or both, could impact the privacy rights protected by the *Charter*. Some aspects of the issues discussed here could also impact freedom of expression or the right against self-incrimination, also protected under the *Charter*.

These issues are complex. Each raises specific concerns about its intersection with considerations of security and individual rights, including privacy. International and economic considerations also come into play.

Challenges

In the physical world, law enforcement and national security agencies use a variety of tools to collect information and evidence to further their investigations and to assist foreign counterparts. The *Criminal Code* and other statutes, such as the *CSIS Act and the Mutual Legal Assistance in Criminal Matters Act*, authorize the use of these tools. For example, investigators at a crime scene may look for physical evidence such as DNA, fingerprints, weapons or other items of importance that may relate to the crime. In the digital world, investigators use other tools to collect digital information and evidence. In the digital world, investigators may be looking for information and evidence (data) such as online addresses (website or IP addresses), the types of communication that took place, with whom, and for how long.

Law enforcement and national security agencies obtain access to such data as authorized by law. However, the legislation providing for certain investigative tools may not be adequate to deal with the complexity, diversity, and rapid pace of change in the digital world. Current challenges impacting investigative capabilities include the following:

- lack of consistent and timely access to **basic subscriber information** to help identify the subscriber to a communications service;

[28] Some of the measures introduced by this Act were new production orders that allow for authority to obtain tracking data, tracing communication, and transmission data, new powers for preservation of data, and the creation of a new offence for the non-consensual distribution of intimate images, known as "revenge porn." The Act also introduced measures to adapt some existing investigative tools to current technology and aligned those changes with privacy safeguards and requirements for judicial oversight.

- lack of consistent and reliable technical **intercept capability** on domestic telecommunication networks;
- diminished ability to investigate due to the use of **encryption**; and
- inconsistent **retention** of communications data.

These challenges are discussed in order below.

In addition, cyberspace is not easily bound by domestic borders and laws. Many communications service providers (CSPs) have no infrastructure or business presence in Canada, but provide Internet-based communications services. These providers operate in Canada but may fall beyond the reach of Canadian law. This can cause significant challenges and delays for law enforcement and national security agencies in acquiring the information necessary to advance investigations. It can also lead to critical intelligence and evidence being unobtainable.

Basic Subscriber Information

Consider a scenario…

There is suspicion that Mr. A. has inspired Mr. M. to begin planning a terrorist attack in Canada with an unidentified person. Much of Mr. M's collaboration happens through exchanges over the Internet, such as through online forums.

As part of the investigation of this suspicious activity, a police officer wants to request the identity (basic subscriber information) related to a particular Internet Protocol (IP) address that has been involved in these online exchanges. However, to get the information from the Internet service provider (ISP), the officer would need a court order. The officer is in the early stages of the investigation and does not have enough information to meet the threshold for obtaining this court order, since getting an order requires more than suspicion that the activities are taking place. As a result, the officer is unable to pursue an investigative lead in a timely and effective manner.

"Basic subscriber information" (BSI) consists of basic identifying information that corresponds to a customer's telecommunications subscription. This can include name, home address, phone number, email address, and/or IP address. BSI does not include the contents of communications. BSI provides law enforcement and national security agencies with key information. This information is particularly useful at the outset of an investigation and may also be used to follow investigative leads. The information allows the police and national security agencies to identify an individual.

In 2014, in *R. v. Spencer*, the Supreme Court of Canada decided that the police could not request the name and address of a person in relation to his or her IP address where it would reveal intimate details of his or her anonymous online activities, except in an emergency situation or pursuant to a reasonable law. The Court concluded that the manner in which the police in this case obtained such information interfered with privacy interests protected by the *Charter*.

Without specific legislation designed to permit access, law enforcement and national security agencies have had difficulty getting timely and effective access to BSI since the *Spencer* decision. As a result, law enforcement agencies have used tools already available in the *Criminal Code*, such as general production orders. These tools are designed for a larger search scope. They are meant for situations such as seeking the complete browsing history, medical records or financial history of an individual. Because of this a high degree of judicial scrutiny is necessary.

The use of these tools for BSI presents the following challenges, especially during early stages of an investigation:

- The information needed to apply for a court order -- for example, a general production order -- may not be available at the beginning of an investigation. The existing information may not attain the threshold required for a court to grant an order.

- The process to obtain a search warrant or a general production order can be slow and involve considerable work and resources. The process has requirements that may be disproportionate when the only information investigators are seeking is BSI, even if the requirements are proportionate in other situations involving greater privacy intrusions.

As a result of these challenges, key evidence may be lost and opportunities to prevent a crime from happening missed. A tool designed to access BSI specifically could, with appropriate safeguards, both enhance investigative capabilities and respect privacy interests.

Laws in many foreign jurisdictions specifically permit law enforcement and national security agencies to obtain BSI. In many cases, this can occur without prior judicial authorization (generally, obtaining BSI without prior judicial authorization is called administrative access). These foreign jurisdictions include the U.S., the UK, Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

The laws and regulations in these jurisdictions vary in how they limit and safeguard administrative access to BSI. Some jurisdictions give certain agencies access to BSI administratively but require other agencies to obtain judicial authorization first. In some cases, a general administrative scheme for obtaining BSI operates, but an order from a judge may be required under certain conditions. These conditions requiring a court order may include when BSI is stored as part of a data retention requirement, or when certain categories of BSI are sought, such as an IP address or other data unique to mobile cellular devices, such as an International Mobile Subscriber Identity (IMSI) number. Other limitations in getting administrative access to BSI include requirements for senior police officers to approve requests and limiting BSI access to certain types of crime, or including prosecutors in the process to obtain some types of BSI.

Any measures to address the need for consistent and timely access to BSI would have to take into consideration the investigative needs of law enforcement and national security agencies and the

impact of those measures on industry. The measures would also have to protect privacy rights in accordance with the *Spencer* decision.

Interception Capability for Communications Services

Law enforcement and national security agencies intercept private communications under the *Criminal Code* and the *CSIS Act* to obtain communications when investigating certain crimes (as listed in the *Criminal Code*) or threats to national security. Each Act sets out procedures to obtain judicial authorization to use interception techniques. These procedures are designed to uphold privacy rights.

Law enforcement and national security agencies obtain the necessary court orders to intercept communications. However, in some cases CSPs may not be able to perform the interception because the technical capability to intercept communications has not been built into their infrastructure. This hinders investigations that are being pursued under judicial authorization. In turn, this can prevent law enforcement and national security agencies from fulfilling their mandates.

Canada does not impose a general legal requirement for CSPs to have interception capabilities on their networks. Many other countries do. Australia, the U.S., the UK and many other European nations require CSPs to have an interception capability. In the U.S., for example, the *Communications Assistance for Law Enforcement Act*, usually referred to as CALEA, imposes this obligation. The U.S. Federal Communications Commission website explains CALEA.[29] Because of CALEA, traditional voice switches in the U.S. today include an intercept feature.

Continuing the scenario from above…

The investigation has now proceeded to a point well beyond suspicion and the police have received an authorization from a judge to intercept the communications of Mr. M.

However, when the police contact the telecommunications service provider, they learn that the service provider has not built a capability to intercept communications into its infrastructure. The service provider cannot complete the work required to develop and implement this intercept capability before the authorization expires. As a result, the police miss out on obtaining key evidence, even though they had court authority to intercept the communications.

Several issues need to be taken into account when discussing whether to require CSPs to introduce intercept capability. These include the impact on privacy, the investigative needs of law enforcement and national security agencies, and how introducing requirements for intercept capability may affect the costs and competitiveness of industry.

[29] https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance

Encryption

Encryption converts a readable electronic message into an unreadable message. To decrypt the message (make it readable again), the reader must use one or more specific decryption "keys." Encryption is widely regarded as a best practice to enhance security and protect privacy online. It is commonly used to protect individual messages, personal devices and transmission channels. Secure encryption is also vital to cybersecurity, e-commerce, data and intellectual property protection, and the commercial interests of the communications industry. Canada's policy on cryptography (established in 1998) underlines the importance of encryption to the viability, stability and growth of the economy and e-marketplace and encourages the use of encryption to protect privacy, personal information and data. Today, free encryption technologies and services are widely available. These include encryption that often operates without the users' knowledge or need to activate it. Encryption technologies may be built in to a user's communication service.

However, encryption technology also helps criminals and terrorists to avoid discovery, investigation and prosecution by making their communications unreadable to investigators. The international availability of encryption tools and the complexities of encryption make law enforcement and national security investigations more difficult. They also pose challenges for law enforcement working with foreign partners in fighting serious international crimes.

It is difficult to address the problematic use of encryption without also reducing its benefits. As a result, very few countries have proceeded to limit encryption through legislation in the interests of protecting law enforcement and national security agency capabilities. This is despite the challenges posed by encryption for law enforcement and national security agencies being well known. Encryption has been the subject of concern and discussion in many jurisdictions since the 1990s.

The UK is among the few countries to impose limits on encryption through law – in this case, the *Regulation of Investigatory Powers Act, 2000*. The Act gives legally authorized persons (such as law enforcement and national security agencies) the authority to serve notices on individuals or bodies requiring the disclosure of protected (for example, encrypted) information in an intelligible form. This can be done through decryption or disclosure of encryption keys that the person is believed to hold. These provisions have attracted controversy.

In the 1990s, a series of legislative initiatives (sometimes referred to as "Clipper Chip" proposals) were suggested in the U.S. to impose built-in decryption capabilities. These proposals were highly controversial and attracted vigorous opposition from privacy and civil liberties groups and from groups concerned about the potential damage to industry. None of these proposals became law. However, vigorous debate about encryption continues in the U.S., as do concerns of law enforcement about encryption. This was seen most recently in the controversy that arose when the U.S. government asked Apple to help it obtain information contained on a phone associated with the San Bernardino terrorist incident.

Continuing the scenario from above…

The police were finally able to develop intercept capability and obtain court authority again to intercept the communications of Mr. M.

To avoid having his plans discovered, however, Mr. M had encrypted his communications, which were unreadable to the police as a result. In addition, the service provider advised the police that it could not help decrypt the communications. After months of investigative delays and despite court authority to intercept the communications of Mr. M, the police cannot read them to obtain potential evidence. As a result, Mr. M's communications remain protected from law enforcement.

Even when law enforcement or national security agencies can intercept a communication, with assistance from a service provider under a court order, the data that is obtained is often unreadable due to the layers of encryption that cannot be decrypted or otherwise removed. Encryption challenges also apply to the court-ordered production of historical data, such as email, text messages, photos and videos from lawfully seized smartphones, computer hard drives and other digital devices. Since encryption can be used by anyone, a private sector organization may not be able to help law enforcement and national security agencies decrypt communications because the organization might not have the technical ability to decrypt material encrypted by someone else.

No provisions specifically designed to compel decryption are found in the *Criminal Code,* the *CSIS Act* or in other Canadian laws. In other words, there is no law in Canada designed to require a person or organization to decrypt their communications.

Discussion about encryption and decryption must take into account the potential impact on the following:

- human rights, including privacy rights, freedom of expression, and the right against self-incrimination;
- the investigative needs of law enforcement and national security agencies;
- commercial interests, such as competitiveness and the protection of intellectual property;
- how compelling decryption could weaken existing IT infrastructure models and systems;
- cybersecurity; and
- e-commerce.

Data Retention

"Data retention" refers to the general requirements to store certain elements of subscribers' telecommunications data, such as telephone numbers dialed, call length, time of call, and Internet equivalents, for the purpose of supporting law enforcement and national security investigations. These data can provide key pieces of information and evidence. Data retention ensures that this

information will be kept for a specified period so that law enforcement and national security agencies can obtain this information with a warrant, if required for an investigation. To date, Canada has not pursued a telecommunications data retention requirement for law enforcement and national security purposes.

Continuing the scenario from above…

As part of its ongoing investigation, the police learn that Mr. M had used his mobile phone over three weeks in July 2015 to communicate with individuals linked to terrorist groups. The police seek a court order to obtain telecommunications data associated with Mr. M's mobile phone account. However, the company keeps records for business purposes only for nine months. As a result, the company has already deleted data from July 2015 and the data are not available to the police.

Parliament recently introduced *preservation* powers into the *Criminal Code* when it enacted the *Protecting Canadians from Online Crime Act*. These powers allow law enforcement agencies to seek a court order or demand the preservation of specific computer data belonging to specific persons for a brief time to assist in investigations.

However, some business practices are changing and companies are deleting data more quickly than before, sometimes before law enforcement can seek a court order for or demand preservation. In addition, the length of time data is held varies from company to company. General data retention requirements would provide for companies to keep data for a standardized period. However, this might mean that companies have to store data for longer than they require strictly for business purposes. Requiring data retention for a given period could also increase risks to personal information held by companies. The longer personal information is kept, the longer it is vulnerable to attack.

General requirements for data retention already exist in some foreign jurisdictions or have been proposed or debated there. In the U.S., some data retention bills have been introduced in Congress, but none have been enacted. Australia recently enacted data retention requirements. On March 15, 2006, the European Union (EU) issued a Data Retention Directive (DRD) to impose data retention requirements for telecommunications data on its member states.

The DRD required that data retention be implemented through legislation enacted by EU member states at the national level. The manner of the implementation varied significantly among member states, in part because of controversy over these requirements in some states. On April 8, 2014, the Court of Justice of the European Union struck down the DRD, calling it inconsistent with privacy rights in Europe.

EU member states are now looking at their respective national laws to determine if and how their national laws on data retention need adjustment after the court decision. Some countries, such as Germany, have already introduced changes. The Federal Constitutional Court of Germany declared

the country's own domestic legislation unconstitutional in March 2010. A new data retention law came into effect in Germany on January 4, 2016. The law introduced many safeguards, such as reducing the obligation to retain data from six months to ten weeks and restricting access to such data to cases involving "serious crimes" only.

The discussion of telecommunications data retention requirements should take into account several issues, including the following:

- the investigative needs of law enforcement and national security agencies;
- the impact on privacy interests; and,
- the impact on the costs and competitiveness of companies resulting from data retention requirements.

What do you think?

How can the Government address challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values, including respect for privacy, provision of security and the protection of economic interests?

In the physical world, if the police obtain a search warrant from a judge to enter your home to conduct an investigation, they are authorized to access your home. How should investigative agencies operate in the digital world?

Currently, investigative agencies have tools in the digital world similar to those in the physical world. As this document shows, there is concern that these tools may not be as effective in the digital world as in the physical world. Should the Government update these tools to better support digital/online investigations?

Is your expectation of privacy different in the digital world than in the physical world?

Basic Subscriber Information (BSI)

Since the *Spencer* decision, police and national security agencies have had difficulty obtaining BSI in a timely and efficient manner. This has limited their ability to carry out their mandates, including law enforcement's investigation of crimes. If the Government developed legislation to respond to this problem, under what circumstances should BSI (such as name, address, telephone number and email address) be available to these agencies? For example, some circumstances may include, but are not limited to: emergency circumstances, to help find a missing person, if there is suspicion of a crime, to further an investigative lead, etc… Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and email address) to be as private as the

contents of your emails? your personal diary? your financial records? your medical records? Why or why not?

Do you see a difference between the police having access to your name, home address and phone number, and the police having access to your Internet address, such as your IP address or email address?

Interception Capability

The Government has made previous attempts to enact interception capability legislation. This legislation would have required domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These legislative proposals were controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it.

Should Canada's laws help to ensure that consistent interception capabilities are available through domestic communications service provider networks when a court order authorizing interception is granted by the courts?

Encryption

If the Government were to consider options to address the challenges encryption poses in law enforcement and national security investigations, in what circumstances, if any, should investigators have the ability to compel individuals or companies to assist with decryption?

How can law enforcement and national security agencies reduce the effectiveness of encryption for individuals and organizations involved in crime or threats to the security of Canada, yet not limit the beneficial uses of encryption by those not involved in illegal activities?

Data Retention

Should the law require Canadian service providers to keep telecommunications data for a certain period to ensure that it is available if law enforcement and national security agencies need it for their investigations and a court authorizes access?

If the Government of Canada were to enact a general data retention requirement, what type of data should be included or excluded? How long should this information be kept?

INTELLIGENCE AND EVIDENCE

National security information needs to be protected from unnecessary public disclosure. At the same time, there is a need to facilitate its use in legal proceedings, when appropriate, while maintaining the fairness of the proceedings and the integrity of the justice system.

The challenge is significant in criminal and related proceedings involving constitutionally protected interests. National security information might also, for example, be important in advancing or defending against a civil case. The Government might also use such information when making administrative decisions, which in turn can be judicially reviewed.

When national security information is involved—or potentially involved—in a legal proceeding, it brings into play issues of fundamental justice, the rule of law and the confidence of Canadians in the justice system. The potential disclosure of national security information may also limit the effectiveness of national security agencies and make it more difficult to assure foreign partners that national security information they have shared with Canada is protected.

Key Principles

The discussion of intelligence and evidence raises several important principles, including the following:

- the requirement that laws be consistent with the *Charter* ;
- the obligation of the Government to protect sensitive sources, capabilities and techniques, and its relationships with international partners, in the interests of national security and international relations;
- the ability of courts and tribunals to consider as much relevant material as possible to ensure that judgments are based on a complete picture of the facts and that justice is done; and
- the need for legislative tools to be flexible enough to apply in a broad range of circumstances.

Section 38 of the *Canada Evidence Act* (CEA) provides the framework for the disclosure and use of national security information in a broad range of legal proceedings. Under section 38, a Federal Court judge must assess whether or not the disclosure would be injurious to international relations, national defence or national security. If disclosure would be injurious, the judge must then consider whether the public interest in disclosure outweighs the public interest in non-disclosure. The process under section 38 of the CEA is conducted in the Federal Court even though, for example, the information may relate to a proceeding in a different court.

This two-part process, also known as a bifurcated process, has been the subject of criticism.

The Supreme Court of Canada concluded that this bifurcated approach is constitutional in a criminal proceeding (*R. v. Ahmad (2011)*). Still, the Court invited the Government to consider its policy choice of using a bifurcated system. The issues surrounding intelligence and evidence have also been addressed in a number of reports, including reports of parliamentary committees and the Air India Inquiry.[30] Intelligence and evidence has also been the subject of consultations in New Zealand and the UK.

Intelligence and evidence issues can be expected to continue to arise for several reasons, including that a number of federal agencies are involved in national security investigations. In some cases, the need for cooperation between federal institutions has resulted in an increasing number of government actions being informed by national security information.

Criminal Proceedings

The Federal Court does not hear criminal cases, unlike the criminal courts in the provinces and territories. However, issues relating to the disclosure of national security information in these cases are largely addressed by Federal Court judges.

This means that, in some instances, the criminal court in a province may be unable to see the national security information and may only be able to rely on unclassified summaries provided by the Federal Court.

In other cases, the Attorney General of Canada, in consultation with investigating agencies, may allow disclosure in court of national security information under certain conditions, determined case by case. However, these proceedings are unable to incorporate the protections for national security information built into the *Canada Evidence Act*. Nor can they benefit from using the Federal Court's secure facilities or relying on its administrative expertise in handling national security information.

Consider a scenario…

After a long investigation, the RCMP lay criminal charges in the superior court of the province against Mr. M for planning a terrorist attack. Information provided by CSIS was essential to the RCMP investigation. This information was obtained from a foreign agency, which provided it on condition that it not be further disclosed without the agency's consent. The foreign agency refuses to consent to the disclosure. Revealing this national security information without the foreign agency's consent would damage CSIS's relationship with it.

To protect against the disclosure of the information provided by the foreign agency, the Attorney General of Canada makes an application under the *Canada Evidence Act* for the Federal Court to decide whether it is in the public interest to protect or disclose the information. The Federal Court judge decides to protect the national security information, which means that the actual information

[30] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

will not be given to the judge of the superior court or be relied on during the prosecution.

However, the judge of the Federal Court also decides to prepare an unclassified summary of the information, which is provided to Mr. M and the judge of the superior court. Mr. M uses this summary to defend himself against the charges and the judge of the superior court may consider it during the proceedings. Because this information is an important part of the prosecution's case, not being able to rely on the complete information in the superior court could cause the prosecution to fail.

National security agencies collect information to advise government, but the information is not generally intended to be used as evidence. In some circumstances, the obligation on the prosecutor to make disclosure in criminal cases may require the prosecutor to approach these agencies to see if they have information relevant to the case. The prosecutor must do this even if the agencies did not provide that information to law enforcement for the criminal investigation. This is one way for national security agencies to get drawn into criminal proceedings.

Potential Impacts on Charter Rights

When trying to protect national security information in a criminal case, the Government must ensure that any measure to do so is consistent with the *Charter*.

An individual accused of a crime has a right to a fair trial, including the right to make full answer and defence. This involves broad access to information that relates to the investigation and charges. The accused also has a right to be present throughout the trial. Finally, the open court principle protected by the *Charter* may come into play when national security information is used in a criminal trial.

Civil Proceedings

National security information may be relevant in a civil proceeding and can sometimes be central to a proceeding. Where national security information is involved, a plaintiff may be unable to make its case, and a defendant may be unable to defend itself, because the information needed to establish the case or defend against a claim needs to be protected. This situation can arise when the federal government is sued for allegedly wrongful conduct, when it is the plaintiff, or in proceedings where the federal government is not at all involved (for example, a dispute between two private companies).

If a judge is unable to take into account the national security information in the civil proceeding, justice may not be served. The lack of relevant information could lead to damage to someone's reputation, costly settlements or loss of public confidence in the legal system.

To protect the national security information from being disclosed to the court and non-governmental parties, the same bifurcated process under the *Canada Evidence Act* described for the criminal process above applies to civil proceedings.

Potential Impacts on Charter Rights

Unlike criminal proceedings, civil proceedings do not automatically bring the *Charter* right to liberty into play. However, parties in civil proceedings generally have a right to documents that contain relevant information that either directly or indirectly advances or damages the case of one party or another. The protection of national security information from disclosure in a civil case could make it difficult to successfully pursue, or defend against, *Charter* claims.

Administrative Proceedings

Many federal administrative decision makers might rely on national security information in their work. These decision makers include federal government officials, ministers, boards and administrative tribunals. The decisions involve a wide variety of matters, such as issuing or revoking permits or licences. For example, decisions about issuing passports are considered administrative proceedings.

As in criminal and civil proceedings, national security information must be protected in administrative and related proceedings, while at the same time the proceedings must ensure fairness. Section 38 of the *Canada Evidence Act* provides a general regime for protecting national security information in some of these situations. Challenges similar to those outlined in the criminal and civil contexts exist here as well.

Apart from section 38 of the *Canada Evidence Act*, a number of specific regimes, varying slightly in their procedures, allow for the protection and use of the national security information during proceedings. Immigration proceedings are one example.

Potential Impacts on Charter Rights

Procedural fairness requirements vary depending on the nature of the administrative decision. The content of the duty of fairness, which includes the rights to know the case to meet and to respond in a meaningful way, varies depending on the rights and interests at stake. Even when *Charter* rights are significantly impacted, the right to know the case to meet is not absolute.

Proceedings under the *Immigration and Refugee Protection Act* (IRPA)

In making immigration decisions, the Government must sometimes rely on classified information (that is, information that if disclosed would be injurious to national security or endanger the safety of a person) to determine whether foreign nationals and permanent residents may enter or remain in Canada (whether they are "admissible"). Division 9 of the IRPA allows the Government to protect and use this information during immigration proceedings. The best known of these Division 9 proceedings are commonly called security certificate proceedings.

The certificate is a document, signed by the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. It states that there are reasonable

grounds to believe that the named person is inadmissible to Canada for reasons of security, violating human or international rights, serious criminality or organized criminality. The certificate is referred to a judge of the Federal Court to determine its reasonableness. The proceedings at the Court have two parts:

(1) public proceedings, where the person named in the certificate, along with their counsel, receive non-classified information and an unclassified summary of the classified information that is part of the certificate; and,
(2) closed proceedings, where the public, the person named in the certificate and their counsel are not present and a court-appointed special advocate (a private lawyer with an appropriate security clearance) receives the classified and non-classified information relevant to the certificate and protects the interests of the named person.

Consider a scenario…

Ms. N is a permanent resident currently in Canada. CSIS has classified information from sources within Canada, as well as from an international partner, that shows Ms. N is part of a terrorist group and a danger to the security of Canada. She has been attending Mr. A's meetings. CSIS provides this information to the Minister of Public Safety and Emergency Preparedness and the Minister of Immigration, Refugees and Citizenship. The ministers decide to sign a security certificate and a warrant for her arrest. The certificate and warrant are filed with the Federal Court. The security certificate process protects the classified information from being disclosed while allowing it to be used by the Federal Court judge, who must determine if the certificate is reasonable.

Potential Impacts on Charter Rights

A person's rights under the *Charter* are engaged by security certificate proceedings. These include the right not to be deprived of liberty and security of the person, except in accordance with the principles of fundamental justice. These principles include the right to a fair hearing, and the right to know the case to meet and to answer that case.

To protect these rights, the law provides certain safeguards. During closed proceedings, special advocates protect the interests of the person named in the certificate. They can challenge government claims that information cannot be disclosed, as well as the relevance, reliability and sufficiency of the information and evidence in the case. Special advocates can make submissions to the Court, cross-examine witnesses during the closed proceedings, and exercise any other power the judge authorizes.

Also, whenever a person is subject to detention or conditions under a warrant, the Court reviews this detention or these conditions on a regular basis (at least once every six months).

Finally, judges ensure the fairness of these proceedings and decide whether the security certificate is reasonable. The Supreme Court of Canada, in the *Harkat* decision, stated that the "judge is intended to play a gatekeeper role, is vested with broad discretion and must ensure not only that the record

supports the reasonableness of the ministers' finding of inadmissibility, but also that the overall process is fair."[31]

The ATA, 2015 changed three aspects of Division 9 of IRPA proceedings (e.g. security certificates):

- The Government can immediately appeal when a judge orders the public disclosure of information that the Government considers must remain classified;
- The information that the ministers must file with the Federal Court is that which is relevant to the ground of inadmissibility on which the certificate is based and which allows the person to be reasonably informed of the case; and,
- The Government may ask the judge for an exemption from providing some classified information to the special advocate (as part of the disclosure of relevant information in closed proceedings). The judge may grant this exemption only if satisfied that the exempted information would not enable the person to be reasonably informed of the Government's case. The judge is permitted to consult with the special advocates about the information before making this decision.

Continuing the scenario from above…

During the security certificate process for Ms. N, the Federal Court judge decides that some of the classified information should be disclosed publicly. The Government appeals this decision immediately because releasing this information would harm national security. The Federal Court of Appeal reviews the decision to disclose the information. The Federal Court of Appeal decides to protect the information and the case continues without it being disclosed.

What are other countries doing?

Australia, New Zealand, the UK and the U.S. face the same challenges of handling intelligence and evidence in their court systems. In criminal matters, for the most part, courts work from legislated roadmaps to protect national security information and maintain an adversarial legal system.

In general, Australia and the U.S. allow private (non-government) counsel to be security-cleared and have access to national security information in representing their clients. New Zealand and the UK have developed surrogates: special counsel acting as alternatives to disclosure of the national security information to the person involved.

In civil litigation involving the potential disclosure of national security information, some countries differ if national security information is sought to be used as evidence. In the U.S., a legal concept known as the common law State Secrets Privilege has evolved. This permits hearings behind closed

[31] *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37.

doors without the affected person or the person's counsel being present which can result in the summary dismissal of claims based on the potential disclosure of state secrets. Elsewhere, including in Australia, procedures established by legislation allow for the substitution of national security information with summaries, admissions of fact or limited disclosure (where possible). Finally, the UK has legislated closed civil proceedings where the judge may review and rely on national security information tendered in closed proceedings, with the interests of the non-government party represented by a special advocate.

Senior administrative tribunals in Australia, the UK and New Zealand consider complaints involving security agencies as a part of their broad supervisory roles. Given their mandate, these senior administrative tribunals involve sitting judges.

What do you think?

Do the current section 38 procedures of the *Canada Evidence Act* properly balance fairness with security in legal proceedings?

Could improvements be made to the existing procedures?

Is there a role for security-cleared lawyers in legal proceedings where national security information is involved, to protect the interests of affected persons in closed proceedings? What should that role be?

Are there any non-legislative measures which could improve both the use and protection of national security information in criminal, civil and administrative proceedings?

How could mechanisms to protect national security information be improved to provide for the protection, as well as the reliance on, this information in all types of legal proceedings? In this context, how can the Government ensure an appropriate balance between protecting national security and respecting the principles of fundamental justice?

Do you think changes made to Division 9 of the IRPA through the ATA, 2015 are appropriately balanced by safeguards, such as special advocates and the role of judges?

CONCLUSION

Canada, like other countries, faces national security threats. The threat of terrorism, by global and by domestic actors, is real and evolving. More people are radicalizing to violence. Some are leaving Canada to join terrorist groups overseas, while others focus their attention on Canada itself. Canadians expect the Government to keep them safe. At the same time, the Government must comply with the rights enshrined in the *Charter*.

The issues described in the Green Paper and this background document relate to major components of our counter-terrorism framework. Some chapters discuss measures already in place. Certain chapters highlight current gaps, while others explain where the Government would like to take action. We hope that this information helps Canadians understand this complex area as we begin consultations with them about how best to respond.

Government counter-terrorism actions undoubtedly impact rights protected under the *Charter*.

Views will differ on what are justifiable and reasonable impacts. There will also be strong opinions on the tools we should employ and how they should be employed.

The views of Canadians about these issues – issues affecting us all – will help inform the Government as it designs the most appropriate mechanisms to deal with the evolving terrorism threat facing Canada.

Thank you for taking the time to read through this paper and for providing your thoughts.

ANNEX – DIAGRAM OF SCENARIO CHARACTERS

The chart below demonstrates Mr. A's links to his followers, and which ones are discussed in various chapters in the document.

Mr. A

Mr. B	Radicalization to violence
Mr. C	Threat reduction
Mr. D	
Mr. F	Domestic national security information sharing
Ms. G	Passenger Protect Program
Mr. I	*Criminal Code* – peace bonds
Ms. J	*Criminal Code* – recognizance with conditions
Ms. K	*Criminal Code* – advocacy or promotion of terrorism offences in general
Ms. K	*Criminal Code* – seizure and forfeiture of terrorist propaganda
Ms. L	Terrorist financing
Mr. M	Investigative capabilities in a digital world
Mr. M	Intelligence and evidence – criminal proceedings
Ms. N	Intelligence and evidence – proceedings under the *Immigration and Refugee Protection Act*

There are also two other individuals, who are not associated to Mr. A, but who appear in some chapters.

Ms. E	Domestic national security information sharing
Mr. H	Passenger Protect Program