CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

CANADIAN CIVIL LIBERTIES ASSOCIATION
Submission to the National Security Consultation
Public Safety Canada and the Department of Justice Canada
December 15, 2016

Canadian Civil Liberties Association
900 Eglinton Ave. E., Suite 900
Toronto, ON M4P 2Y3
Phone: 416-363-0321
www.ccla.org

Contents

OVERVIEW

The Canadian Civil Liberties Association ("CCLA") provides these submissions to Public Safety Canada and the Department of Justice Canada, in response to the government's public consultation on Canada's national security framework, drawn from issues outlined in the government's National Security Green Paper, 2016[1].

At the outset, CCLA reiterates that we reject any paradigm that pits security against human rights and civil liberties, or asks for a 'trade-off' of rights for security. Rather, CCLA believes that rights and liberties and security are part of the "same seamless web of protection"; we believe that civil liberties and human rights are prerequisites for effective security and public safety, and not impediments. Rights failures and information sharing failures resulted in tragic consequences for all 329 people killed in the bombing of Air India flight 182; for Maher Arar; and for Abdullah Almalki, Ahmad Abou-Elmaati, and Muayyed Nurredin. We urge the government to seriously consider and implement the recommendations, and (in the case of the the Iacobbucci Inquiry the observations) of the three Federal Commissions of Inquiry of these respective cases.

As an overarching comment, the CCLA has serious concerns regarding accountability deficits in Canada's national security framework, which we regret to observe, have continued to expand – and not shrink – with the steady proliferation of new national security laws and policies since 2001. Notwithstanding lessons from the recommendations and observations of three Federal Commissions of Inquiry (Arar 2006, Iacobucci 2008, and Air India 2010) – each of which involved acts or omissions Canada's national security and intelligence communities which contributed to tragic consequences to individuals – Canada's national security and intelligence communities have continued to enjoy new and broader powers without legally binding measures to ensure the tragic mistakes of the past are not repeated, and without any commensurate increase in accountability. The most recent law – the *Anti-terrorism Act, 2015* (i.e. Bill C-51)- is fraught with such broad and sweeping powers, and with such serious accountability deficiencies, that it in our view imperils long-term effective security of Canada, and simultaneously undermines the constitutional rights and liberties which act as safeguards for our democracy. At no time since Bill C-51 was introduced have we been provided with concrete evidence as to where the previous legislative and policy regimes specifically failed – rather Bill C-51 has introduced new overbroad unjustified powers across the whole of government that has a national security mandate.

The CCLA filed a *constitutional challenge* to the *Anti-terrorism Act, 2015* in July 2015. At the time that CCLA filed that Challenge in Ontario's Superior Court of Justice, CCLA's Executive Director and General Counsel stated that:

> [The *ATA, 2015*] creates broad and dangerous new powers, without commensurate accountability, and this can result in serious mistakes. Some of the powers granted by Bill C-

[1] Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, (Background Document), (Ottawa: 2016), online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx#fn30-rf> [Green Paper].

51 are secretive in nature, so the public may never know if and when Canadians' rights are being violated, though individuals will be faced with the fallout.

CCLA's challenge specifically addressed our concerns regarding failures of constitutional safeguards regarding CSIS; the new Security of Canada Information Sharing Act (SCISA); amendments impeding disclosure to special advocates in security certificate cases, in the Immigration and Refugee Protection Act (IRPA); the procedural failures regarding the Passenger Protect Program and the No Fly List; and amendments to the Criminal Code. In early 2016, we decided to seek to hold the challenge in abeyance (i.e. temporary) pending outcome of promises by the newly elected Federal Government of Canada to take steps to address national security. CCLA seeks clear, substantive, and timely government responses to the issues we raise in these submissions -- which responses we hope will be the outcome of the consultation process.

In this submission CCLA documents the many changes required not just to the *ATA, 2015*, but more broadly to our national security infrastructure, policies and practices, in order to ensure that rights and security co-exist in Canada.

Accountability

It is the position of the CCLA that effective national security accountability mechanisms are a prerequisite for efficacious security. Without accountability there has been and will continue to be mistakes, misuses, and abuses of power that result in harm to innocent persons, and that place Canada's security in jeopardy.

The *ATA, 2015* increased the scope and sweep of Canada's national security powers, without any commensurate increase in accountability mechanisms. The problem is compounded given that Canada's pre-2015 national security structures were seriously deficient in effective accountability. Furthermore, the recommendations and observations of three Federal Commissions of Inquiry have not been adequately implemented leaving open the possibility for future mistakes and corresponding tragedy.

CCLA draws to the Government's attention the serious accountability deficits we document in our *Charter* Challenge; it is a recurring and ongoing theme running throughout our application that extensive expansion of powers—pursuant to the amendments to the CSIS Act, the Immigration and Refugee Protection Act, and the Criminal Code; and enactment of the Security of Canada Information Sharing Act, and the Secure Air Travel Act—are devoid of appropriate accountability mechanisms and adequate safeguards.

CCLA recommends integrated investigations by national security review bodies or, ideally, a consolidated, enhanced expert review body with robust access to secret information; an independent monitor of national security laws; and independent oversight and review mechanisms for all national security agencies (including the Canada Border Services Agency). We agree with the recent iteration of these positions by Professors Roach and Forcese in their paper addressing

national security accountability, "Bridging the National Security Gap: A three part system to modernize Canada's inadequate review of national security."[2]

Bill C-22's introduction of a Committee of Parliamentarians attempts to rectify this accountability deficit, but the substantial limits on the Committee will render the body less effectual than Canada requires and Canadians deserve. Recent proposed amendments to allow the Committee access to secret information is a good step. We further recommend removing or substantially restricting the government's broad power to halt Committee investigations and information requests.

Threat Reduction

The *CSIS Act* amendments represent a seismic shift in both CSIS's powers, and the way it may carry out its functions. As we argue in our *Charter* Challenge to the *ATA, 2015*, the new CSIS provision which can be interpreted as enabling courts to issue warrants in violation of the law or the *Charter* is a radical proposition that is directly contrary to the rule of law, constitutional supremacy, and the independence of the judiciary. Moreover, by giving CSIS police-like powers to "disrupt" perceived security threats, the CSIS amendments remove longstanding protections against a covert and largely unchecked security intelligence agency intervening in, and often interfering with, everyday policing matters.

We recommend repealing CSIS's new warrant provisions and disruption powers.

Domestic National Security Information Sharing

CCLA has long argued that proper information sharing is necessary for effective national security. This is consistent with the findings of the Arar and Air India Commissions of Inquiry. Information sharing must be targeted, accurate, and effective, and compliant with the constitutional and human rights principles of 'necessity, proportionality, and minimal impairment'. This is best achieved by ensuring that there are adequate safeguards regarding reliability of the information, as well as strict caveats on use, accessibility, dissemination, retention and destruction of that information. These safeguards are missing in the *Security of Canada Information Sharing Act* (the "*SCISA*").

The *SCISA* vastly expands the scope and scale of information that may be shared across government institutions, in a manner that is not restricted to constitutional principles of necessity, proportionality, or minimal impairment. CCLA's *Charter* Challenge addresses those parts of section 2 of the *Anti-terrorism Act, 2015* enacting sections 2, 5 and 6 of the *SCISA*, which CCLA claimed violate sections 2, 7 and 8 of the *Charter* in a manner that cannot be saved by section 1.

To address the problems with the *SCISA*, the unconstitutionally vague and overbroad definition of "activity that undermines the security of Canada" must be clarified to prevent information about law-abiding, innocent Canadians from being caught in the sweeping regime.

In general, the restrictions on the use, dissemination and destruction of shared information under the *SCISA* are woefully lacking, ignorant of the lessons of the Arar Commission of Inquiry, and in need of extensive revision. CCLA supports the recommendation of the Arar Commission of Inquiry

[2] Craig Forcese & Kent Roach, "Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security", *Ottawa Faculty of Law Working Paper No. 2016-05* (31 March 2016), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714498>.

that the Government require information sharing be subject to written agreements and caveats, which CCLA recommends contain restrictions on lawful use and destruction of the information.

The existing mechanisms, such as the Office of the Privacy Commissioner and the Auditor General do not have the mandate or powers required to provide sufficient accountability for the *SCISA*. The Arar Inquiry Policy Review recommendations should be adopted to remedy the dearth of accountability and oversight for the *SCISA* and to facilitate integrated review among agencies.

To help facilitate review of information sharing under the *SCISA*, the Government should introduce regulations mandating record-keeping for disclosures under the *SCISA*. This is an essential step in ensuring effective review of the regime and the ability of Canadians to challenge improper information sharing.

CCLA recognizes that information sharing can be an indispensable tool in countering terrorism. But safeguards respecting necessity, proportionality and minimal impairment should be incorporated into the *SCISA*. To that end, it is important that information only be shared with agencies or departments with mandates connected to that information, and information should only be shared in accordance with the principles of reliability, necessity and relevance.

The Passenger Protect Program

The new *Secure Air Travel Act* ("*SATA*") gives the Passenger Protect Program ("PPP") its own legal basis and framework. In principle, this is positive and CCLA has long recommended a clear legislative basis for the program. Unfortunately, as currently codified, the *SATA* does not accomplish this goal. As we argue in our *Charter* challenge to the *ATA, 2015*, SATA unconstitutionally violates individuals' *Charter* rights to mobility and due process.

Moreover, even if the government's commitment to improving the redress process related to the PPP is effective and fixes the real problem of false positives to the list, these improvements are insufficient to address the PPP's violation of individuals' *Charter* rights.

Criminal Code Terrorism Measures

The amendments to the *Criminal Code* introduced by the *ATA, 2015* are overbroad, unnecessary and accordingly unjustified. The offence of promoting or advocating terrorism offences in general is not needed, given the already wide range of existing criminal terrorism offences. As we argue in our *Charter* challenge to the *ATA, 2015*, the offence is unconstitutional because it is unnecessary, overbroad and disproportionate, and further is likely to chill legitimate dissent.

The new terrorist propaganda provisions give rise to similar concerns of vagueness, overbreadth, and unjustified restrictions of free expression. These new *Criminal Code* provisions make terror suspects harder to detect and investigate. Further, the lower thresholds for preventive arrest, detention and recognizances with conditions – already exceptional broad powers – are now amplified and undermine due process rights and the rule of law.

Investigative Capabilities in a Digital World

CCLA is concerned that questions of expanding state surveillance and policing powers have been introduced into this consultation with insufficient context or public education on complex issues and unfamiliar technologies.

We believe that prior to increasing or changing investigative capabilities, Canadians need access to an evidence-based analysis of the actual risks to public safety from changing technologies, which must include an assessment of whether problems identified are potentially based in lack of training or resources. We need to consider not just what police would like, but what we, as a society, think is necessary and proportionate to legitimate risks.

Furthermore, CCLA respectfully submits that the challenge the Canadian government faces should be seen to be as much about regulating the use of intrusive new surveillance technology as it is about creating new kinds of access to Canadian's personal information via legislation. Investigative agencies should operate in the digital world as they are required to operate in the physical world: in accordance with law and with respect for our *Constitution* and our *Charter of Rights and Freedoms*.

The Green Paper discusses the following investigative tools in particular: lawful access to basic subscriber information without a warrant, mandated interception capabilities and retention requirements, and compelled decryption. CCLA presents reasons why all of these tools are problematic at best, and unconstitutional at worst.

Principles are not—and should not be--affected by platform. And regardless of the existence of a rich record of the activities most of us engage in daily that is facilitated by technology, most people do not expect that the state will, or should, have unhindered access to these records.

Intelligence and Evidence

In our *Charter* Challenge, CCLA submits that in particular, the amendments under sections 83(1) and 85.4(1) which permit the Minister of Public Safety and Emergency Preparedness to withhold information from special advocates appointed to protect the rights of individuals subject to security certificates violate section 7 of the *Charter*.

In general, the CCLA is seriously concerned that the lessons regarding intelligence and evidence identified by the Air India Commission of Inquiry are absent from the *ATA, 2015* and indeed the Green Paper. CCLA reiterates the need for greater accountability measures in national security policies and practices. Increased accountability, through independent, security-cleared bodies, could improve the protection and use of national security information in criminal, civil and administrative proceedings, while respecting individuals' rights and freedoms.

INTRODUCTION

About the CCLA

The Canadian Civil Liberties Association (CCLA) is a national, non-profit, non-partisan, non-governmental organization supported by thousands of individuals and organizations from all walks of life. The CCLA was constituted in 1964 to promote respect for and observance of fundamental human rights and civil liberties and to defend and foster the recognition of those rights and liberties. CCLA's major objectives include the promotion and legal protection of individual freedom and dignity. For over 50 years, CCLA has worked to advance rights, freedoms and justice throughout Canada, through litigation and regularly appearing before all levels of court, engaging in advocacy, and in public education through interaction with the media, holding public events and speaking in schools.

About this submission

CCLA provides this submission to Public Safety Canada and the Department of Justice Canada, with respect to the public consultation on national security.

CCLA has longstanding concerns regarding national security policy and practice in Canada. We have been speaking out on the gaps in national security accountability since well before the introduction of Bill C-51, now the *Anti-terrorism Act, 2015 (ATA, 2015)*. We have participated in many fora on this topic from the time that Bill C-51 was proposed, up to and including various opportunities provided by the current consultation process. These submissions include, but are not limited to:

- Written and oral submissions to the Senate Committee on National Security and Defence regarding the CBSA and accountability, April 2014
- Written and oral submissions to the Standing Committee on Public Safety and National Security regarding Bill C-51, March 2015
- Written and oral submissions to the Senate Committee on National Security and Defence regarding Bill C-51, April 2015
- Written and oral submissions to the UN Human Rights Committee during the Sixth Periodic Report of Canada, including concerns about national security accountability and Bill C-51, June 2015
- Participation in the national security roundtable convened by Ministers Goodale and Raybould-Wilson, October 2016
- Participation in the national security consultation town hall, hosted by the Standing Committee on Public Safety and national Security, Toronto, October 2016
- Oral submissions to the Standing Committee on Access to Information, Privacy and Ethics, regarding the *Security of Canada Information Sharing Act*, November 2016
- Participation in a national security consultation at the Munk School, University of Toronto, November 2016

We have also taken action in the courts. CCLA filed a *Charter* Challenge to specific sections of the *Anti-terrorism Act, 2015* on July 21, 2015 in the Ontario Superior Court of Justice. CCLA's action is

currently pending, and we remain concerned that the deficiencies we identify in that challenge have not yet been addressed.

While we appreciate the professed commitment of the new government to address deficiencies in Canada's national security framework -- including the introduction of Bill C-22 and the launching of the present consultation -- the accountability gaps in our national security infrastructure, and the lack of *Charter* compliance in the *ATA, 2015* remain outstanding. Furthermore, the CCLA is seriously concerned that the tone of the Green Paper, despite some references to rights, creates a narrative skewed in favour of professed "needs" of national security agencies and law enforcement. The Green Paper in many instances positions rights as barriers to necessary change, rather than recognize that rights are fundamental protections inherently necessary to an effective security regime, in a democratic state. The Green Paper fails to present the problematic aspects of the ATA, 2015 in a manner that identifies both the potential advantages and risks, to invite debate. The Green Paper also goes well beyond the *ATA, 2015* to reopen closed questions about expanding state surveillance and investigatory powers, under the heading "Investigative Capabilities in a Digital World." We are disappointed that questions of lawful access, warrantless access, and compelled decryption are introduced into this consultation in a manner that fails to adequately contextualise them within the long history of their debate—and past rejection—in Canada. We further believe that the Green Paper fails to provide Canadians with the rich and nuanced information that is necessary if they are to be expected to supply informed feedback to this consultation.

This submission reiterates and builds upon the positions we have consistently taken in relation to the changes made through Bill C-51, now the *Anti-terrorism Act, 2015*[3] to Canada's national security laws, and addresses new issues raised in this current consultation process.

For each section of this submission, we explicitly raise the lack of *Charter* compliance of specific parts of the *Anti-terrorism Act, 2015* that CCLA has identified in our *Charter* Challenge, and then respond to the questions asked in the consultation background document, "Our Security, Our Rights: National Security Green Paper, 2016"[4] to elucidate the manner in which we think the deficiencies we identify in our *Charter* Challenge must be addressed.

At the time that CCLA filed our *Charter* Challenge to the newly passed *Anti-terrorism Act, 2015*, CCLA's Executive Director and General Counsel made the following statement:

> [The *ATA, 2015*] creates broad and dangerous new powers, without commensurate accountability, and this can result in serious mistakes. Some of the powers granted by Bill C-51 are secretive in nature, so the public may never know if and when Canadians' rights are being violated, though individuals will be faced with the fallout.

More than a year later, we continue to believe that the Act is fundamentally flawed, and reiterate our concern that despite our calls, we have not presented with concrete evidence that it was

[3] *Anti-terrorism Act, 2015*, S.C. 2015, c. 20 [*ATA, 2015*].
[4] Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016*, (Background Document), (Ottawa: 2016), online: <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx#fn30-rf> [Green Paper].

necessary. Our submission outlines changes required not just to the *ATA, 2015*, but more broadly to our national security infrastructure, policies, and practice are situated in a rights-compliant construct that can best ensure effective, efficacious security and public safety.

1. Accountability

GREEN PAPER QUESTIONS:

- *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 [Canadian Border Services Agency]?*
- *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?*

SECTION SUMMARY

The significant overhaul to Canada's national security system resulting from the passing of the *ATA, 2015* increased agency powers, but contained no commensurate increase in accountability mechanisms. This problem is exacerbated because Canada's existing national security structures in sum are seriously deficient in meaningful or effective accountability. The need for greater accountability in this area has been recognized in federal Commissions of Inquiry, two of which have made considered and detailed recommendations based on extensive study, research, and expert consultation. Accountability not only prevents human rights abuses but it is a prerequisite for efficacious security.

As set out in CCLA *Charter* Challenge, expansion of powers – for example, pursuant to amendments to the the *CSIS Act*, the *Immigration and Refugee Protection Act*, the *Security of Canada Information Sharing Act*, the *Secure Air Travel Act,* and the *Criminal Code*—have been enacted without appropriate accountability measures or adequate safeguards.

CCLA does believe that the CRCC, OCSEC and SIRC should have expanded powers to review and investigate complaints against their respective agencies. CCLA is particularly concerned that these entities should be properly resourced to enable effective, comprehensive and thorough review of their respective agencies – which we understand does not currently exist. Further, necessary and sufficient resourcing of review agencies will allow effective collaboration.

CCLA recommends integrated investigations by national security review bodies or, ideally, a consolidated, enhanced expert review body with robust access to secret information; an independent monitor of national security laws; and independent oversight and review mechanisms for all national security agencies (including the Canada Border Services Agency). We agree with the

recent iteration of these positions by Professors Roach and Forcese in their paper addressing national security accountability, "Bridging the National Security Gap: A three part system to modernize Canada's inadequate review of national security."[5]

Bill C-22's introduction of a Committee of Parliamentarians attempts to rectify this accountability deficit, but the substantial limits on the Committee will render the body less effectual than Canada requires and Canadians deserve. Recent proposed amendments to allow the Committee access to secret information is a good step. We further recommend removing or substantially restricting the government's broad power to halt Committee investigations and information requests.

SUBMISSION

CCLA's Charter Challenge

CCLA's concerns about accountability gaps and failures are evident in our Charter challenge to the ATA, 2015. Throughout our challenge we set out our concerns to the amendments to the *CSIS Act*, the IRPA, the Criminal Code, and enactment of the in the *Security of Canada Information Sharing Act*, and the *Secure Air Travel Act.* Our concerns stem from increases in scope and scale of powers and discretion without commensurate accountability mechanisms or regard for constitutional safeguards. Accountability, we should emphasise, is not just a matter of oversight or review, it is also about the ways in which legal safeguards are implemented into systems to prevent mistakes, to identify mistakes and to ensure that recourse and redress is provided if mistakes do occur. In the national security context, mistakes can have devastating consequences.

For example, in the *CSIS Act* Amendments, our challenge points out that the proposed judicial warrant process will happen *in camera*, on an *ex parte* basis, with no adversarial challenge, no prospect of appeal, and no requirement that the actions taken by CSIS be disclosed after the passage of time to the individual targeted. While we acknowledge that the Government has stated they will make sure warrants are not issued that permit non-compliance with the *Charter*, the entire process as it is formulated in the Act lacks safeguards to ensure that CSIS gives full and frank disclosure to the judge, as well as lacking due process safeguards protecting the rights of targeted individuals.

In the *Security of Canada Information Sharing Act*, the concept of "activity that undermines the security of Canada" is unconstitutionally vague, and the processes by which that standard will be applied are completely opaque to those whose information may be shared. Individuals have no possible recourse, because they have no realistic ability to learn that their information has been shared or to question the legitimacy of that sharing. No review body has jurisdiction to review the vast majority of the agencies that the Act empowers to share information.

In the *Secure Air Travel Act*, individuals are placed on the list on mere suspicion—"reasonable grounds to suspect"—that they may threaten transportation security, right to appeal the Minister's decision is narrow, the process is burdensome, and the Act does not provide for the appointment of a special advocate to protect the rights of the listed individual in secret hearings.

---

[5] Craig Forcese & Kent Roach, "Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security", *Ottawa Faculty of Law Working Paper No. 2016-05* (31 March 2016), online: SSRN <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2714498>.

Overview: accountability is essential and currently inadequate

In 1981, the Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, more colloquially known as the McDonald Commission, wrote:

> Maintaining an acceptable system of government control and review of security and intelligence activities poses a serious challenge to a democracy. Among these activities, those related to security must, in particular, often be conducted with great secrecy. Therefore, it may be difficult to provide direction and control in a manner which is consistent with the principles of democratic government. We perceive the difficulties, but we do not concede that the principles must be compromised. Where a choice must be made between efficiency in collecting intelligence and the fundamental principles of our system of government, the latter must prevail. It would be a serious mistake - indeed a tragic misjudgment - to compromise our system of democratic and constitutional government in order to gather information about threats to that system: this would be to opt for a cure worse than the disease.[6]

As the Commission so persuasively explained, oversight and accountability for national intelligence activities is difficult but nonetheless absolutely and fundamentally essential in a democratic society. In Canada, it is also elusive and arguably illusory. Ever since the McDonald Commission, experts (and subsequent Commissions of Inquiry including most notably the O'Connor Commission), have called for a stronger accountability framework for Canada's national security apparatus. Those calls have consistently fallen on deaf ears. In fact, in 2012 Prime Minister Harper took a step in the other direction and reduced CSIS oversight, abolishing the office of the Inspector General, which was responsible for ensuring the Minister was properly informed about CSIS's activities. Unfortunately, in light of the significant revisions to Canada's national security system that occurred with the passage of Bill C-51 the need has become more urgent than ever to improve oversight and review for our spy agencies.[7] The new *ATA, 2015* substantially increases the powers of state agencies but fails to commensurately increase accountability mechanisms. This failure not only puts human rights at risk, but may also actually imperil effective security operations which may suffer from a lack of the 'big picture' perspective that ongoing oversight and thorough review can provide.

As CCLA has publicly stated on many occasions, the Committee of Parliamentarians put forward in Bill C-22 is a necessary start to filling the accountability gaps in our national security infrastructure, but it is not in itself sufficient. It is from this perspective that we respond to the Green Paper questions below.

---

[6] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police, *Part VIII: A Plan for the Future: Direction and Review of the Security Intelligence System* (1981) at 841, online: Library and Archives Canada <http://epe.lac-bac.gc.ca/100/200/301/pco-bcp/commissions-ef/mcdonald1979-81-eng/mcdonald1979-81-report2/mcdonald1979-81-report2-vol2-eng/mcdonald1979-81-report2-vol2-part2-eng.pdf>.

[7] Forcese and Roach draw our attention to the distinction between 'oversight' which is usually an executive branch function and occurs as events unfold, and 'review' which is an audit of past performance to ensure legal and policy compliance. See Craig Forcese, Kent Roach & Leah Sheriff, *Bill C-51 Backgrounder #5: Oversight and Review: Turning Accountability Gaps into Canyons?* (27 February 2015) online: SSRN <https://ssrn.com/abstract=2571245> or <http://craigforcese.squarespace.com/national-security-law-blog/?currentPage=4>.

Existing review bodies should have greater capacity in general, as well as to review and investigate complaints against their respective agencies

The Green Paper asks whether existing review bodies require greater capacity to review and investigate complaints, but CCLA would like to respectfully suggest that these bodies could be substantially strengthened in ways beyond their ability to investigate complaints. We will briefly address issues with each review body below.

OCSEC

The CSE Commissioner's functions under the *National Defence Act* include review to ensure compliance with the law, investigating complaints against the CSE, and informing the Minister of any incidences of non-compliance with the law. This includes verifying that CSE takes sufficient measures to protect the privacy of Canadians. However the CCLA has expressed its concerns that questioning "lawfulness" of CSE activities has been a matter of statutory interpretation of the *National Defence Act* – compliance with an arguably outdated, broadly-worded statute does not ensure compliance with human rights principles.

It is CCLA's position that the CSE must carry out its functions and operations with a commitment to upholding fundamental privacy rights and principles including necessity and proportionality. The capabilities of modern technologies which allow mass surveillances and mass capture, storage and uses of the personal identifying information of innocent law-abiding Canadians, should not be permitted to override fundamental human rights principles. Strengthening the OCSEC is necessary to enhance Canadian's ability to trust that the CSE is using its great powers proportionately, effectively, and lawfully.

In particular, CCLA highlights the deficiencies in CSE accountability as follows:

- CSE does not have meaningful public accountability, as it does not officially report to Parliament. The Office of the CSE Commissioner delivers its review report in classified form to the Minister of Defense, with a redacted version delivered to Parliament.

- As is the case with Security Intelligence Review Committee, the CSE Commissioner's office is small in relation to the size of the organisation it reviews. The Commissioner has a staff of 11. The CSE Commissioner has recently gone on record, in his 2015-2016 Report on Plans and Priorities, as expressing concern about the adequacy of his resources in relation to his workload and responsibilities.

- Finally, the Commissioner does not make legal determinations, nor does he act in place of a court of law; what this means is that he judges CSE's actions on the basis of their interpretation of the law, not his own. Or as one Commissioner stated: "With respect to my reviews of CSE activities carried out under ministerial authorization, I note that I concluded on their lawfulness in light of the Department of Department of Justice interpretation of the applicable legislative provisions."[8] This is particularly problematic since Canadians are not privy to these interpretations.

In addition to addressing these accountability gaps, CCLA would like to highlight one proposal that is not addressed in the Green Paper. The Government indicated in its election platform that it will "limit Communications Security Establishment's powers by requiring a warrant to engage in the surveillance of Canadians."[9] We encourage the Government to keep this promise.

CCRC

On March 6th, 2013, Bill C-42 was passed, which made amendments to the *RCMP Act* to strengthen the Royal Canadian Mounted Police review and complaints mechanism and to implement a framework to handle investigations of serious incidents involving RCMP employees.[10] The Act established a new complaints commission, the Civilian Review and Complaints Commission for the

---

[8] Office of the Communications Security Establishment Commissioner of Canada (2006), *Annual Report 2005-2006* (Ottawa: Minister of Public Works and Government Services Canada, April 2006), online: OCSEC <https://www.ocsec-bccst.gc.ca/s21/s46/s11/eng/2005-2006-annual-report>; Office of the Communications Security Establishment Commissioner of Canada (2013), *Annual Report 2012-2013* (Ottawa: Minister of Public Works and Government Services Canada, June 2013), online: OCSEC <https://www.ocsec-bccst.gc.ca/s21/s46/s18/eng/2012-2013-annual-report>.

[9] Liberal Party of Canada, "Chapter 4: A Strong Canada", *Real Change: A New Plan for a Strong Middle Class* (2015) at 53, online: <https://www.liberal.ca/files/2015/10/New-plan-for-a-strong-middle-class.pdf>.

[10] *Enhancing Royal Canadian Mounted Police Accountability Act*, S.C. 2013, c. 18, online: <http://laws-lois.justice.gc.ca/eng/annualstatutes/2013_18/index.html>, see also: <http://openparliament.ca/bills/41-1/C-42/>.

Royal Canadian Mounted Police ("CRCC"). However, the amendments do not implement three of the recommendations of the O'Connor policy review, namely that the new commission be able to examine the compliance of the RCMP's activities with "international obligations" and "the standards of propriety expected in Canadian society"; have the power, on the request of the Governor in Council, to conduct reviews of the activities relating to the national security of one or more federal departments, agencies, employees and contractors; and review the national security activities of the Canada Border Services Agency.

We would also note that the amendments expand the circumstances under which hearings may be held in private, including a catch-all provision that provides the Commission with a broad discretionary power to hold *in camera* proceedings if privileged information will likely be revealed during the hearing or if "it is otherwise required by the circumstances of the case".[11] In addition, the amendments permit the Commission to hold an *ex parte, in camera* hearing in the absence of one of the parties in order to protect sensitive information. Thus, while the Commission is granted supremacy and exclusive jurisdiction to conduct investigations into certain activities of the RCMP, it has been provided with wider discretion to conduct its reviews in secret. Moreover, the revised *RCMP Act* does not incorporate Justice O'Connor's suggestion to allow the commission to appoint an independent counsel to determine the need to maintain the confidentiality of certain information and hear representations made on behalf of the excluded parties, thus ensuring a proper balance between the need for confidentiality and transparency. The conclusions issued by the commission following an investigation are not subject to appeal or review by any court and they do not specifically mention the right to seek judicial review under the *Federal Courts Act*.[12] These deficiencies should be addressed.

SIRC

The Security Intelligence Review Committee's ("SIRC") 2015-2016 Annual Report raised the need for permanent and secure funding commitments to keep pace with the increasing workload that is created by the expansion of CSIS's powers under the *ATA, 2015*. Given the importance of SIRC's role and the potential for an expansion in complaints as well as an increased need for review in light of the changes made by the *ATA, 2015*, CCLA encourages provision of stable and sufficient resources to the SIRC.

Existing review bodies should be mandated to collaborate on reviews

Following 9/11, Canada's national security agencies have been acting in an increasingly integrated manner, but with no corresponding integrated accountability for their actions. These accountability deficits are amplified by the increase in integration and information sharing between Canada's agencies with foreign agencies, as well as with foreign and domestic private actors. The existing review bodies are limited in the scope of what they can do by silos that do not match the increasingly integrated nature of national security activities, and there is no review at all for many agencies that are now involved in national security work. In such a landscape the potential for human rights mistakes and national security failures is increasing.

The need for integrated oversight and review of national security functions was identified in the recommendations of the Arar Commission of Inquiry, and the findings of the Air India Commission

[11] *Royal Canadian Mounted Police Act*, R.S.C., 1985, c. R-10, s. 45.1(2)(d).

[12] Lyne Casavant & Dominique Valiquet, "Bill C-42: An Act to amend the Royal Canadian Mounted Police Act and to make related and consequential amendments to other Acts", The Library of Parliament, *Publication No. 41-1-C42-E*, (10 September 2012), (Revised 7 November 2012), at 19.

of Inquiry, but that advice has not been followed. Almost ten years ago Justice O'Connor of the Arar Inquiry recognized the significant mismatch between the growth and integration of national security operations and concomitant deficiencies in accountability.

> Among the more significant changes have been enhanced information sharing, new legal powers and responsibilities, and increased integration in national security policing[13].

He went on to recommend a new review body for the RCMP, named the Independent Complaints and National Security Review Agency for the RCMP ("ICRA"), with enhanced powers and authority to consider the RCMP's national security operations in addition to its other work. Justice O'Connor noted that many other agencies with national security responsibilities do not have independent review, including Canada Border Services Agency ("CBSA"), Citizenship and Immigration Canada ("CIC"), Transport Canada, the Financial Transactions and Reports Analysis Centre of Canada ("FINTRAC") and Foreign Affairs.

With respect to these five entities, he notes:

> The national security activities of the five entities in question are integrated to a significant degree with those of the RCMP. Integration of national security activities is a critical component of Canadian policy, and co-operation among Canadian agencies involved with national security should be encouraged. However, effective review of RCMP national security activities that are integrated with those of the five entities requires that the latter's activities be subject to a similar type of review. Otherwise, there is a serious potential for gaps in accountability for integrated national security activities and inconsistent or incoherent results in the review of the same activities.[14]

As a result, Justice O'Connor recommended that ICRA review the CBSA and SIRC review CIC, Transport Canada, FINTRAC and Foreign Affairs with respect to national security functions. Coupled with this is a recommendation to create "statutory gateways" allowing review bodies to work together in order to break through their silos. These gateways would allow sharing of information, co-ordination of activities, joint investigations and other forms of co-operation between SIRC, ICRA and OCSEC. In addition, an Integrated National Security Review Coordinating Committee ("INSRCC") was recommended to bring together the heads of the three review bodies to facilitate cooperation, report to government on accountability issues as well as the impacts of national security practices on human rights and freedoms.

On this latter point, the experience of the United States may be helpful. In 2004 the Privacy and Civil Liberties Oversight Board was created with whole-of-government authority to examine and provide advice on privacy and civil liberties impacts of terrorism policies. The United Kingdom has also recently introduced a Privacy and Civil Liberties Board. Furthermore, Canada's allies do not seem as limited by silos in terms of accountability, with review agencies in the United Kingdom, Australia and New Zealand having the ability to examine a broad range of national security activities.

The Arar Inquiry's recommendations were made almost a decade ago, and while the creation of the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police ("CRCC") is a step forward, other recommendations remain unaddressed. This shortcoming was highlighted by

---

[13] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Policy Review), (Ottawa: Public Works and Government Services Canada, 2006) at 18, online: Library and Archives Canada <http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/EnglishReportDec122006.pdf> [Arar Inquiry, Policy Review].

[14] *Ibid*, Arar Inquiry, Policy Review, at 21.

the United Nations Committee Against Torture ("UNCAT") when it expressed concern that the Arar Inquiry recommendations on accountability were not implemented. The UNCAT recommended that Canada "consider urgently implementing the model for oversight of agencies involved in national security agencies, proposed by the Arar Inquiry".[15]

While the Arar Inquiry's strong recommendations would have served Canada well if implemented at the time, CCLA believes that even more is required today given the significant growth in national security operations and mandates over the last ten years. In fact, Justice O'Connor's words calling for reform of national security review in 2006 are a reminder that Canada needs significant and immediate reform of its national security sector review.

> The national security landscape in Canada is constantly evolving to keep abreast of threats to our national security. It is vital that review and accountability mechanisms keep pace with operational changes.[16]

The review bodies have requested increased integration themselves. With respect to CSIS, SIRC has repeatedly raised concerns regarding its constraints in adequately exercising its mandate. The CSE Commissioner has similarly remarked upon the difficulties inherent in reviewing CSE's functions given its inability to engage in review of other institutions with which CSE regularly collaborates. This collaboration is likely to increase in light of the provisions in the *ATA, 2015*. Mandating—not just permitting—collaboration on reviews is an appropriate and necessary step forward for improved accountability. Please refer as well to our comments above on page 10-11, and below, regarding an independent monitor/National Security Advisor for national security activities.

Independent review mechanisms of other departments and agencies that have national security responsibilities, such as the CBSA [Canadian Border Services Agency] should be introduced

There are numerous federal departments and agencies in Canada with national security responsibilities, and also federal, provincial and municipal police forces with such responsibilities. The plethora of powers and actors that forms Canada's national security landscape – powers that are significantly enhanced by the *ATA, 2015* – urgently demand commensurate accountability mechanisms.

Our foremost concern relates to the absence of any appropriate and independent review mechanism for the CBSA, an agency that enjoys sweeping powers including law enforcement powers. CBSA officers can arrest, with or without warrants, permanent residents or foreigners if they believe these individuals pose a threat to public safety, or are illegally in the country -- i.e. inadmissible. CBSA also has the power to detain foreigners and permanent residents, including asylum seekers. The CBSA works closely with the RCMP and CSIS in information sharing that the CBSA may rely upon in determining who may be a threat or who may be illegally in the country. Indeed, as Justice O'Connor noted, the CBSA "prevents entry by people not legally allowed into Canada (inadmissible persons), collects intelligence, and detects, arrests, detains and removes people who are in Canada illegally." CBSA also engages in information collection and dissemination with foreign agencies, with impact upon the actions (decisions, conclusions, investigations, apprehensions) of individuals within its jurisdiction.

---

[15] Committee Against Torture, *Report of the Committee Against Torture*, UNCATOR, 67th Sess., Supp. No. 44, UN Doc. A/67/44 (2012), online: Office of the United Nations High Commissioner for Human Rights <http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=A%2f67%2f44&Lang=en>.

[16] Arar Inquiry, Policy Review, *supra* note 13, at 22.

These wide powers of the CBSA are highly intrusive and coercive, and have the impact to seriously, adversely and deleteriously affect the lives of individuals. They must be subject to independent review in order to ensure they comply with Canadian constitutional safeguards, and also the relevant legal obligations binding upon Canada pursuant to international law.

As noted above, Justice O'Connor recommended in his second report pursuant to the auspices of the Arar Commission, that there should be an independent review body for the CBSA, with powers that include complaints investigation and the ability for self-initiated review, including review their law enforcement powers (arrest, detention, and removal) as well as their intelligence gathering powers. His recommendation saw this review as falling to the same body that he recommended be created to review the RCMPs national security activities. A more recent proposal is that in Senate Bill S-205, which has proposed an Inspector General of the Canada Border Services Agency. While the exact form the independent review body should take is open for discussion, the need to move quickly to introduce strong CBSA oversight should not be.

The CCLA strongly recommends that independent review of CBSA be implemented without delay. We cannot underscore enough the importance, in a free and democratic society, of the principles of accountability and transparency, secured through independent review, of power. Nor can we understate the concomitant dangers posed to human rights and dignity – including to life, to liberty, to security of the person – by unchecked power.

There is a need for an independent review body to look at national security activities across government

CCLA recommends that there should be a central, coordinating position, which, as Professors Forcese and Roach have pointed out, might fit naturally into the role of the National Security Advisor. The holder of this position would have the specific responsibility to ensure coordination and integration of operational activities while ensuring that appropriate policies and practices are in place across agencies – a job made particularly necessary by the expansion of CSIS powers which may overlap with RCMP investigations, and by the greatly expanded information sharing provisions in the *ATA, 2015.* The idea of having the National Security Advisor play a strategic, co-ordinating and oversight role was also a recommendation of the Air India Inquiry.[17]

CCLA further recommends the creation of a single integrated review body, mandated to review all of the government's national security activities, with powers to investigate complaints, self-initiate investigations, and make recommendations for reform. This body must be resourced at a level commensurate with its responsibilities. Some have called such a body a "super SIRC." The scope of this body's mandate should encompass review of the work of CSIS, CSE, CBSA, RCMP, FINTRAC, CIC, Foreign Affairs and others identified as relevant during expert consultation.

This recommendation is in addition to Bill C-22's all-party committee of Parliamentarians with whole-of-government responsibilities, access to secret information and the ability to monitor the integrated activities of all agencies with national security roles.

---

[17] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy, The Relationship Between Intelligence and Evidence and the Challenges of Terrorism Prosecutions*, vol. 3, (Ottawa: Public Works and Government Services, 2010) at 193, (Commissioner: Major J.), online: Library and Archives Canada <http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/volume3/volume3.pdf> [Air India Inquiry, Final Report].

Other measures needed to increase parliamentary accountability for the ATA, 2015

CCLA supports a mandatory statutory review of the *ATA, 2015* after three years.

In addition, we recommend that the Government undertake a comprehensive, public review of the *ATA* examining its compliance with the Canadian *Charter of Rights and Freedoms*[18] (the "*Charter*"). Many experts expressed serious concerns about *Charter* compliance during the debates around Bill C-51, but these concerns were not addressed prior to passing the Bill. As we have noted, and will continue to emphasise, CCLA responded with a *Charter* challenge before the Ontario Superior Court that lays out 5 particular areas of concern in relation to (1) the *CSIS Act*[19], (2) the *Immigration and Refugee Protection Act* ("*IRPA*")[20], and (3) the *Criminal Code*[21] with respect to "advocating or promoting terrorism". The challenge also addresses (4) the new *Secure Air Travel Act*[22] ("*SATA*") as well as (5) the new *Security of Canada Information Sharing Act*[23] ("*SCISA*"). We acknowledge and appreciate the government statement that it will ensure all CSIS activities comply with the *Charter,* but we would like to see that promise extended to all aspects of the *ATA*.

In April 2016, during initial parliamentary debate, the Minister of Justice released a "*Charter* impacts" analysis of Bill C-14**,** the government's physician assisted dying legislation. While the statement did not fully provide the comprehensive analysis that we believe parliamentarians and Canadians need to consider before bills become law, it set an excellent precedent that we believe should be followed in future.

CCLA believes that the government of Canada should conduct a genuine and thorough legal review of the *ATA* with attention to *Charter* issues. Further, the process by which this takes place, and the results, should be public and transparent. This review should begin by addressing the specific points raised in our Challenge.

2. Threat Reduction

GREEN PAPER QUESTIONS

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?*

[18] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 [*Charter*].
[19] *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23 [*CSIS Act*].
[20] *Immigration and Refugee Protection Act*, S.C. 2001, c. 27 [*IRPA*].
[21] *Criminal Code,* R.S.C. 1985, c. C-46, s. 83.221(1) [*Criminal Code*].
[22] *Secure Air Travel Act*, S.C. 2015, c. 20, s. 11 [*SATA*].
[23] *Security of Canada Information Sharing Act*, S.C. 2015, c. 20, s. 2 [*SCISA*].

- *The Government has committed to ensuring that all CSIS activities comply with the Charter. Should subsection 12.1(3) of the CSIS Act*[24] *be amended to make it clear that CSIS warrants can never violate the Charter? What alternatives might the Government consider?*

SECTION SUMMARY

The *CSIS Act* amendments represent a seismic shift in both CSIS's powers, and the way it may carry out its functions. As we argue in our *Charter* challenge to the *ATA, 2015*, the new CSIS provision giving courts license to issue warrants in violation of the law or the *Charter* is a radical proposition that is directly contrary to the rule of law and the role of the judiciary. Moreover, by giving CSIS police-like powers to "disrupt" perceived security threats, the CSIS amendments remove longstanding protections against a covert and largely unchecked security intelligence agency intervening in, and often interfering with, everyday policing matters.

We recommend repealing CSIS's new threat reduction mandate, including the new warrant provisions.

SUBMISSION

CCLA's Charter Challenge

In our *Charter* challenge to the *ATA, 2015*, the CCLA has argued that new Federal Court judicial warrant process that preauthorizes CSIS to take 'measures that violate Canadian law and the constitutional rights of individuals is unconstitutional. The problems with this new warrant process are several. This warrant application occurs *in camera*, on an *ex parte* basis, with no adversarial challenge, with no prospect of appeal, and with no requirement that the actions taken by CSIS be disclosed after the passage of time to the individual targeted. The Act does not provide for the appointment of a special advocate or an *amicus curiae* to represent the interests of the individual whose *Charter* rights are at stake. It constitutes an extraordinary inversion of the traditional role of the judiciary and the principles of fundamental justice by asking the judiciary, and not Parliament, to authorize limits on *Charter* rights as opposed to protecting such rights and preventing their violation.

As such, and for reasons elaborated upon below, Sections 12.1(3) and 211 of the amended *CSIS Act* unjustifiably violate the liberty and security of person rights guaranteed under section 7 of the *Charter* in a manner that is not in accordance with the principles of fundamental justice. The provisions also violate the principles of judicial independence and impartiality and the separation of powers established by the *Constitution Act, 1867*.

CSIS's new threat reduction mandate is unjustified and overbroad and should be repealed

CCLA has serious concerns about the expanded powers of CSIS, and the lack of commensurate accountability, that were codified in the *CSIS Act* via Bills C-51 and C-44. These changes represent a significant restructuring of Canada's intelligence and security architecture. While the Green Paper notes that CSIS's threat reduction mandate was the subject of extensive public debate prior to

[24] Subsection 12.1(3) of the *CSIS 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…."

passage, the overhaul was nevertheless undertaken without meaningful study and absent significant public or parliamentary input. The *CSIS Act* amendments largely ignore recommendations made by both the Air India and Arar Commissions of Inquiry that point to the desirability of clear demarcation of mandates and powers of agencies, the need for better coordination between agencies, and the concerning accountability deficits in the national security realm. Meaningful reforms to both oversight and review mechanisms are critical and yet were completely absent in CSIS's major overhaul. Finally, the proposed new Committee of Parliamentarians, as presently constituted, is far too ineffectual to provide the necessary oversight and review mechanisms to remedy this oversight and review deficit.

CSIS was originally created as a response to illegal acts and wrongdoings by the RCMP, acts and wrongdoings that were made possible and exacerbated by the RCMP's historical fusion of intelligence and law enforcement powers. In response to these illegal acts and wrongdoings, the McDonald Commission recommended, after extensive study, that law enforcement and intelligence functions be separate. CSIS was thus created as an institution designed to provide sensitive intelligence functions without the threat of these functions being wed to "disruptive" powers.

The *CSIS Act* amendments undermine this careful division of intelligence and law enforcement functions. They expand CSIS beyond a recipient and analyst of human intelligence into an agency with powers to act in Canada and abroad, without regard to international law or foreign domestic law.

This bold and radical restructuring is also at odds with Arar and Air India Commissions of Inquiry which exhaustively reviewed the functions of Canada's national security agencies with consideration to the powers, mandate and actions of CSIS. While these Commissions considered the merits of distinctions between intelligence and law enforcement functions, these distinctions were not found to hamper Canada's counter-terror efficacy.

The CSIA Act amendments represent a fundamental shift in how CSIS will operate, stacking greater powers onto their existing intelligence-gathering functions. The new provisions allow CSIS to take "measures" to reduce threats to the security of Canada. While this language may initially sound benign, the outer limits of these "measures" suggest that CSIS will have a very large sphere in which to operate. In particular, the sole constraints on measures that CSIS may take relate to causing death or bodily harm, obstructing justice, or violating the sexual integrity of an individual. As such, a reasonable interpretation of these provisions is that other violations of law are contemplated as measures open to CSIS, in Canada and abroad.

There has yet to be adequate explanation as to why these "measures" are necessary in order for CSIS to be effective in countering terrorism. As discussed further throughout these submissions, this expansion is particularly troubling in light of deficiencies in the existing and proposed accountability regimes and given that CSIS largely operates in secret.

The new warrant power should be repealed as it interferes with the role of the judiciary and the capacity for effective review

One of the most concerning provisions of the *ATA* is its new warrant power found at s. 12.1(3) of the *CSIS Act*. According to this new provision, measures that CSIS may take to reduce a threat to the security of Canada may not contravene a right or freedom guaranteed by the *Charter* or be in contravention of other Canadian law, *unless authorized by a warrant issued under proposed s. 21.1*. A reasonable interpretation of this language is that the provision permits judges to grant a warrant that authorizes breaches of the law, including the Constitution of Canada.

At present, this is a shocking provision and of serious concern to a society committed to rule of law and constitutional supremacy. Further, the new warrant power turns the role of the judiciary – sworn to uphold the law and ensure that government actors comply with the *Charter* – into a complicit actor to flout rule of law.

As noted in the Green Paper, the present Government has committed to ensuring that all CSIS activities comply with the *Charter.* CCLA expects the government to make good on its guarantee to ensure that all CSIS warrants comply with the *Charter*. This guarantee, if it is to be meaningful, must include a repeal of the new provision authorizing violations of the *Charter* via warrant.

Nevertheless, a repeal of the clause authorizing *Charter* violations is insufficient to remedy this radical and arguably unlawful provision. Even an amended provision is incompatible with the legal responsibilities of a judge insofar as it compels judges to issue warrants to act outside of the law.

Further, warrant applications are on an *ex parte* basis, and brought *in camera,* meaning there is no real check on CSIS in seeking these warrants. The judge does not have the benefit of an adversarial process and is not in a position to test the evidentiary basis for the warrant that is sought. The Federal Court has recently raised concerns that CSIS failed to meet its duty of candour in seeking out a warrant,[25] thus heightening the concerns about the secret warrant process and undermining the faith of Canadians in our security services. Further, individuals who are subject to measures authorized by such warrants may never know this, and therefore will not be in a position to challenge the warrant or the reasons upon which the warrant was authorized. The potential threat of harms from secrecy in this process is exacerbated by the absence of any transparency or accountability safeguards.

Warrants exist to ensure compliance with legal protections, and in the case of section 8 of the *Charter*, to ensure that the search warrant guards against an 'unreasonable search'; i.e. that in the circumstances the search is reasonable. The warrant scheme proposed as worded in s. 12(3) directs the issuance of judicial warrants to authorize CSIS to take measures to reduce a threat to Canada *even if* those "measures will contravene a right or freedom guaranteed by the *Charter* or will be contrary to other Canadian law." In our view, this is unacceptable and contrary to this nation's commitment to constitutional supremacy and rule of law.

The concerns with the new warrant power extend beyond CSIS, as a judge may order "any person" to provide assistance if their assistance may reasonably be considered to be required to give effect to a warrant. This provision could lead a range of government actors (whether or not traditionally operating in the national security realm) to become involved in covert activities and also contemplates involving private individuals in carrying out such covert "measures". Those authorized to take measures pursuant to a warrant may also take it upon themselves to request assistance from "another person". Extending the powers to take "measures" beyond even those within CSIS is deeply concerning and operates without any meaningful checks or balances.

Threat reduction powers are best safeguarded by making them exclusive to the RCMP

The Government Green Paper argues that because the RCMP and CSIS have "different priorities, different approaches, access to different information and a different international presence", there

[25] *X (Re)*, 2013 FC 1275, aff'd 2014 FCA 249.

are crime-prevention situations where CSIS is better placed to disrupt security threats as compared to the RCMP. The *CSIS Act* amendments are intended to achieve this goal.

This justification rings hollow, and will continue to ring hollow, until the government is able to provide the Canadian public with sufficient evidence and transparency to support these claims. On their face, the *CSIS Act* amendments serve to undermine a crucial long-term national security goal: the criminal prosecution of individuals committing terrorist offences. For instance, CSIS' new "disruption" powers have the potential to interfere with ongoing RCMP investigations and to create unnecessary friction between two agencies with different mandates. Because CSIS does not share the RCMP's institutional concerns regarding terrorist prosecutions, it is more likely to taint potential evidence or otherwise undermine criminal investigations of terrorist threats via pre-emptive "disruptive" actions – a difficulty that is exacerbated by a law passed in 2015 that privileges CSIS' human informants, thereby allowing them to avoid testifying in terrorism prosecutions.

It bears emphasizing that the Green Paper justification for the *CSIS Act* amendments was already contemplated and rejected by two of the most comprehensive government-led reviews of Canada's national security framework: the Air India and Arar Commissions of Inquiry. Both Commissions of Inquiry recommended an alternative approach to addressing national security threats, one that is consistent with our *Charter* rights and freedoms: a clearer demarcation of mandates and powers of agencies; better coordination between agencies; and increased accountability measures in the national security realm. The CCLA submits that the government should heed the national security recommendations forwarded by its own Commissions of Inquiry.

3. Domestic National Security Information Sharing

GREEN PAPER QUESTIONS

- *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?*

SECTION SUMMARY

CCLA has long stated that proper information sharing is necessary for effective national security. This is consistent with the findings of the Arar and Air India Commissions of Inquiry. Information sharing must be targeted, accurate and effective, and compliant with the constitutional and human rights principles of 'necessity, proportionality, and minimal impairment'. This is best

achieved by ensuring that there are adequate safeguards regarding reliability of the information, as well as strict caveats on use, accessibility, dissemination, retention and destruction of that information. These safeguards are missing in the *Security of Canada Information Sharing Act* (the "*SCISA*").

The *SCISA* vastly expands the scope and scale of information that may be shared across government institutions, in a manner that is not restricted to constitutional principles of necessity, proportionality, or minimal impairment. CCLA's *Charter* Challenge addresses those parts of section 2 of the *Anti-terrorism Act, 2015* enacting sections 2, 5 and 6 of the *SCISA*, which CCLA claimed violate sections 2, 7 and 8 of the *Charter* in a manner that cannot be saved by section 1.

To address the problems with the *SCISA*, the unconstitutionally vague and overbroad definition of "activity that undermines the security of Canada" must be clarified to prevent information about law-abiding, innocent Canadians from being caught in the sweeping regime.

In general, the restrictions on the use, dissemination and destruction of shared information under the *SCISA* are woefully lacking, ignorant of the lessons of the Arar Commission of Inquiry, and in need of extensive revision. CCLA supports the recommendation of the Arar Commission of Inquiry that the Government require information sharing be subject to written agreements and caveats, which CCLA recommends contain restrictions on lawful use and destruction of the information.

The existing mechanisms, such as the Office of the Privacy Commissioner and the Auditor General do not have the mandate or powers required to provide sufficient accountability for the *SCISA*. The Arar Inquiry Policy Review recommendations should be adopted to remedy the dearth of accountability and oversight for the *SCISA* and to facilitate integrated review among agencies.

To help facilitate review of information sharing under the *SCISA*, the Government should introduce regulations mandating record-keeping for disclosures under the *SCISA*. This is an essential step in ensuring effective review of the regime and the ability of Canadians to challenge improper information sharing.

CCLA recognizes that information sharing can be an indispensable tool in countering terrorism. But safeguards respecting necessity, proportionality and minimal impairment should be incorporated into the *SCISA*. To that end, it is important that information only be shared with agencies or departments with mandates connected to that information, and information should only be shared in accordance with the principles of reliability, necessity and relevance.

SUBMISSION

CCLA's Charter Challenge

In our *Charter* challenge, CCLA notes that the information subject to sharing under the *SCISA* implicates section 7 of the *Charter* as a result of the prejudicial impact information sharing may have on the liberty and security of the person interests of individuals. CCLA argues that "activity that undermines the security of Canada" is an unconstitutionally vague definition that can impact individuals' section 7 security and liberty rights.[26] As the scheme is currently structured, violations can occur without the knowledge of an affected person. Even if there is knowledge, without an appropriate review structure, there can be no effective complaint system, given the absence of any one review structure with jurisdiction to review all the agencies empowered to share information.

[26] *Charter* Application, *supra* note 30, at paras. 32-33.

Further, the scope of information sharing that the SCISA authorises will chill expression and association rights guaranteed by section 2 of the *Charter*, not least because no person is able to determine (or challenge in any meaningful way) how their activities and conduct have been or might be construed by the state as "undermining the security of Canada."

A person will not know that information about, or related to them has been shared, and will have no opportunity to bring a court proceeding in which the Act might then be interpreted. Even assuming an individual has sufficient knowledge to bring a complaint, there is no overarching review body to review the agencies who may share information under the Act, and no ability for existing review bodies to coordinate reviews. Effectively, they are deprived of both recourse and remedy, in the event that information exempted from the scope of the Act is illegally shared.

As per the Supreme Court of Canada's decision in *R. v. Morgentaler*, [1988] 1 SCR 30, no defence should be illusory, or so difficult to attain that it is practically illusory, yet this is the situation created by SCISA. The information sharing also clearly implicates information protected by section 8 of the *Charter* within the meaning of *R v. Wakeling*, [2014] 3 SCR 549. It permits a form of disclosure of this information that is unreasonable, within the meaning of section 8, given the absence of sufficient review and independent checks and balances on this sharing.

The SCISA's overly broad definition of "activity that undermines the security of Canada" should be revised

The definition of "activity that undermines the security of Canada" should be further clarified. As it is, the *SCISA* provides for unprecedented collection and dissemination of information across state agencies, without enforceable privacy safeguards and without limiting the collection of information to 'terrorist activities'.[27] As such, information on law-abiding, innocent Canadians can be swept up in this vast net that is not limited to national security structures. This sets the stage for mass surveillance, profiling and big data analytics. There is significant potential for abuse and harm.

The *SCISA* authorizes information sharing between Government of Canada institutions on any "activity that undermines the security of Canada".[28] This term is defined in section 2 of the *SCISA,* but in a manner that is both vast and uncertain, especially when read in association with the operative parts of the *Act*, in particular, sections 5 and 6. For example, section 5 of the *SCISA* only authorizes disclosure between certain government institutions where such disclosure is not prohibited by law, but this authorization is tied to the definition of "activities that undermine the security of Canada".[29] In CCLA's *Charter* challenge[30] to the *ATA*, CCLA explains that the scope of the information sharing is overbroad and vast – defined by exceptionally broad and concerning language:

---

[27] See *SCISA*, *supra* note 23, s. 5(1): "relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.".

[28] *Ibid*, *SCISA*, s. 2.

[29] *Ibid*, *SCISA*, s. 5.

[30] Canadian Civil Liberties Association, "Issued Notice of Application", at para. 32, online: CCLA <https://ccla.org/cclanewsite/wp-content/uploads/2015/08/Issued-Notice-of-Application-Bill-C-51-C1383715xA0E3A.pdf>. See also Canadian Civil Liberties Association, "CCLA & CJFE mounting Charter challenge against Bill C-51", (21 July 2015), online: CCLA <https://ccla.org/ccla-and-cjfe-mounting-charter-challenge-against-bill-c-51/> [*Charter* Application].

"***activity that undermines the security of Canada*** means any activity, including any of the following activities, if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada:

> (a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;
>
> (b) changing or unduly influencing a government in Canada by force or unlawful means;
>
> (c) espionage, sabotage or covert foreign-influenced activities;
>
> (d) terrorism;
>
> (e) proliferation of nuclear, chemical, radiological or biological weapons;
>
> (f) interference with critical infrastructure;
>
> (g) interference with the global information infrastructure, as defined in section 273.61 of the National Defence Act;
>
> (h) an activity that causes serious harm to a person or their property because of that person's association with Canada; and
>
> (i) an activity that takes place in Canada and undermines the security of another state.

For greater certainty, it does not include advocacy, protest, dissent and artistic expression..

Such a mass scope does not result in meaningful security benefits. Rather, it treats all Canadians as potential suspects—with no thresholds of reasonable suspicion of illegality and/or targeted surveillance—instead of law-abiding citizens who require protection not only from terrorist threats and acts, but also protection of their rights and liberties. This is one of the reasons that further clarification is required. Contrary to the Government's commitment not to limit lawful protest and advocacy, the astoundingly overbroad definition, as it is now, can capture all sorts of unnecessary and disproportionate information on legitimate activities. For example, the definition of "activity that undermines the security of Canada" appears to allow information sharing in relation to legitimate protest activities related to Canada's environmental practices, municipal development activities, international trade agreements, labour disputes, Aboriginal land claims, and a variety of other areas. The definitional base of the *SCISA* is sweeping in its scope and gives rise to genuine concerns about the protection of privacy and the level of intrusion Canadians should reasonably have to tolerate from their government. As such, this and other overbroad aspects of the legislation should be reviewed and revised.

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

In general, the restrictions on the use, dissemination and destruction of shared information under the *SCISA* are blind to the lessons of the Arar Commission of Inquiry, and in need of extensive clarification and revision.

CCLA supports the Arar Commission of Inquiry's recommendation that the Government make information sharing subject to written agreements and caveats.[31] CCLA recognizes these as important safeguards in the collection and exchange of personal information, particularly in the national security context. CCLA recommends that the written agreements also contain the parameters of use and destruction, which would help to clarify the restrictions on the use of shared information by recipient institutions. CCLA is seriously concerned that there is inadequate regard in the *SCISA* to such safeguards; there is no requirement for written agreements.

Although the *SCISA* includes a set of guiding principles for information sharing, these principles are not translated into enforceable provisions in the *Act*. Moreover, the operational parts of the *SCISA* in some cases directly contradict the principles. Significantly, one of the guiding principles is that "respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing",[32] and yet the provisions of the *SCISA* do nothing to facilitate the use of caveats or promote the importance of originator control.

Since the *SCISA*'s minimal constraints on when information can be shared ("in accordance with the law") are not clearly defined, they are hollow limitations. These restrictions should be further clarified, as there is great potential for error and harm to law-abiding, innocent Canadians. While the amendment[33] to section 6 of the *SCISA*, which calls for the use and further disclosure of information to be in accordance with existing "legal requirements, restrictions, and prohibitions", appears on its face to recognize the importance of compliance with lawful protections, scrutiny reveals that there are currently insufficient legally enforceable protections in place, notwithstanding the clear recommendations of the Arar Inquiry report.

The *SCISA* superimposes a new layer of information sharing without commensurate safeguards. It fails to incorporate the lessons of the Arar Commission of Inquiry, while simultaneously increasing the scale and scope of information flow. It is CCLA's view that the *SCISA*'s provisions are reckless and may contribute to serious errors that are compounded in the national security context. Clarifying existing restrictions and making information sharing subject to written agreements and caveats is the first step to appropriately safeguarding information being shared under the *SCISA*. However, this alone will not alleviate CCLA's serious concerns over the dearth of accountability for national security information sharing.

Existing review mechanisms, such as the authority of the Privacy Commissioner to conduct reviews, do not provide sufficient accountability for the SCISA

The existing review mechanisms do not provide sufficient accountability for the overbroad *SCISA*, and the Act itself lacks meaningful accountability or oversight mechanisms for national security information sharing. In fact, the scope and scale of information sharing under the *SCISA* widen the already existing accountability chasms, enabling operations that are inconsistent with democratic principles of transparency and accountability.

---

[31] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (in relation to the Factual Background), (Ottawa: Public Works and Government Services Canada, 2006), Recommendation 9, at 339-42, 366-67, online: Library and Archives Canada <http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf> [Arar Inquiry, Report].

[32] *SCISA*, *supra* note 27, s. 4(b).

[33] A shift from the *SCISA*'s original language permitting further disclosure and use of already shared information "to any person, for any purpose" (*ibid*, s. 6).

Although proper information sharing is necessary for effective national security, ensuring that there are adequate safeguards regarding reliability of the information, as well as strict caveats on use, accessibility, dissemination, retention and destruction of that information, is crucial. These safeguards are missing in the *SCISA* and absent in the Green Paper.

Because of the inherent secrecy that necessarily accompanies national security information, information will often be shared without the knowledge of the subject, meaning that harms to an individual can be perpetuated secretly. As such, a robust complaints and self-initiating review mechanism is necessary, as well as a robust oversight mechanism. Given the civil immunity for so-called 'good faith' disclosures,[34] there is an absence of meaningful legal recourse or redress in the *SCISA*. Further, as observed by the Arar Commission of Inquiry, increasingly integrated operations of national security agencies call for an integrated review process.[35] The international information flow structures in which Canada is an active participant serve to amplify these needs. But these increased and integrated information collection and sharing powers are not matched by increased and integrated review structures, and this is of grave concern to the CCLA.

As CCLA has observed in its *Charter* application, assuming an individual has sufficient knowledge of government information sharing to bring a complaint, which often may not be the case, there is no specialized national security review body with the jurisdiction or mandate to oversee the vast majority of the agencies that the *SCISA* empowers to share information. In its application, CCLA argues that, given the lack of review and demonstrable checks and balances on information sharing under the *SCISA*, such disclosures are *prima facie* "unreasonable", according to the interpretation of that term in *R. v. Wakeling*[36] and, therefore, are contrary to section 8 of the *Charter*.[37]

At the time of its passage, it was suggested that the authority of the Privacy Commissioner and the Auditor General to conduct reviews is sufficient accountability for the *SCISA.* This is inaccurate. The scope and scale of information, as well as the agencies and institutions engaged, are beyond the mandates and resources of either entity: neither having the necessary jurisdiction or powers to review information sharing under the *SCISA*.

Although the Office of the Privacy Commissioner ("OPC") has an "all of government" remit, it is not equipped for reviewing national security information-sharing, and its mandate over personal information is too narrow in the face of "big data" information processing.[38] The OPC itself recognized its limitations in this regard early on, and has called for significant reforms to ensure adequate protections for privacy in the national security context.[39] The OPC's most recent annual report investigated activities under the *SCISA* and raised a range of concerns, including a lack of privacy impact assessments for departments receiving information and poor instructions to front-line staff making the decisions about what information to flag for their supervisors to consider

---

[34] *Ibid*, *SCISA*, s. 9.
[35] Arar Inquiry, Policy Review, *supra* note 13, Recommendation 11, at 582. See generally Arar Inquiry, Policy Review at 19, 522, 580-90.
[36] 2014 SCC 72, [2014] 3 SCR 549 at para. 81, Moldaver J [*Wakeling*].
[37] *Charter* Application, *supra* note 30, at paras. 33-37.
[38] As argued by CCLA in its *Charter* Application, *ibid*, at para. 35.
[39] Office of the Privacy Commissioner of Canada, *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (Ottawa: Minister of Public Services and Procurement Canada, 28 January 2014), online: <https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/201314/sr_cic/>. See also Office of the Privacy Commissioner of Canada, *Statement from the Privacy Commissioner of Canada following the tabling of Bill C-51* (30 January 2015), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2015/s-d_150130/>.

sharing.[40] This confirms the validity of the concerns expressed by CCLA about the lack of built-in safeguards and checks and balances under the *SCISA*.

Even the three existing review bodies for CSIS, the CSE, and the RCMP have no powers to compel the government to follow specific interpretations of the law;[41] the Privacy Commissioner similarly lacks this power.[42] Further, the three review bodies cannot share confidential information with each other or the Privacy Commissioner, nor are they permitted to follow the thread of information sharing beyond the specific agencies under their purview. These limitations prevent joint, coordinated reviews and inter-agency investigation.

Given that the existing review mechanisms do not provide sufficient accountability for the wide-ranging information sharing enabled by the *SCISA*, CCLA proposes the adoption of Justice O'Connor's Arar Inquiry Policy Review recommendations regarding an integrated review scheme. The Commission provided a clear roadmap for effective review, through the creation of "statutory gateways" among national security review bodies to penetrate existing accountability silos among agencies and facilitate integrated review.[43] This included an Independent Complaints and National Security Review Agency for the RCMP.[44] CCLA has long argued that the implementation of the Arar Inquiry recommendations for necessary oversight and integrated review[45] are indispensable to our democracy and for efficacious security.

The Government should introduce regulations requiring institutions to keep a record of disclosures under the SCISA

The Government should indeed introduce legally enforceable regulations requiring institutions to keep a record of disclosures under the *SCISA*. CCLA submits that the secrecy under which the program currently operates renders defense against illegal sharing illusory – if Canadians do not know what is being shared or with whom, mistakes will go undetected because it will be impossible to know whether improper information sharing caused the problem. As CCLA submitted in its *Charter* challenge, the Supreme Court of Canada in *R. v. Morgentaler*[46] stated that no defence should be illusory, or so difficult to attain that it is practically illusory.[47]

In its *Charter* challenge, CCLA argues that there is no serious prospect that anyone outside the SECTION branch knows how the vague concept of "activity that undermines the security of Canada" is being applied. This is because the *SCISA* lacks a mechanism by which people can become aware that information about, or related to them, has been shared, and, therefore, have no opportunity to bring a court proceeding in which the Act might then be interpreted.[48] CCLA further argues that the

---

[40] Office of the Privacy Commissioner of Canada, *2015-2016 Annual Report to Parliament on the* Personal Information Protection and Electronic Documents *Act and the* Privacy Act, (Ottawa: Minister of Public Services and Procurement Canada, September 2016), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516/>.
[41] See *Charter* Application, *supra* note 30, at para. 35.
[42] As argued in CCLA's *Charter* Application, *ibid*, at para. 33.
[43] Arar Inquiry, Policy Review, *supra* note 13, at 583. See generally Recommendation 11, at 585-590.
[44] *Ibid*, Arar Inquiry, Policy Review, at 19, 603. See generally Recommendation 2, at 505-516.
[45] Arar Inquiry, Report, *supra* note 31, Recommendations 6-10 broadly, regarding the need for oversight in information sharing, at 331-343. See generally Arar Inquiry, Policy Review, *supra* note 13, Recommendations 1-13, at 503-607, discussing the need for an integrated review mechanism capable of investigating and reporting on complaints and generating self-initiated review of Canada's national security agencies.
[46] [1988] 1 SCR 30, 63 OR (2d) 281.
[47] *Charter* Application, *supra* note 30, at para. 36.
[48] *Ibid*, *Charter* Application, at para. 33.

lack of any avenue to determine or meaningfully challenge whether their activities have been interpreted as "undermining the security of Canada" will have a chilling effect, deterring legitimate expression and association, contrary to section 2 of the *Charter*.[49]

While clarifying the definition of "activity that undermines the security of Canada", as recommended further above, may help, that change alone is insufficient. Flaws in the *SCISA* also engage section 8 of the *Charter*, which protects against unreasonable search and seizure. Since the *SCISA* lacks review and demonstrable checks and balances, disclosures under the Act are inherently unreasonable, as outlined by the Supreme Court of Canada in *Wakeling*.

Instituting a recording regulation for disclosures is a necessary step in establishing an effective review mechanism that would pass *Charter* scrutiny. Unlike the *SCISA* guidelines, the requirement to keep a record of disclosures must have legal force. The records should state the nature of the disclosure and the reasons for it, so that it can be subsequently reviewed by an oversight body and/or investigated, in the event of a complaint.

This recommendation goes hand-in-hand with the suggestion further above about implementing written agreements and caveats on information being shared.

The SCISA should be clearer about the requirements for listing potential recipients and the list of eligible recipients should be reduced

CCLA is concerned about the general lack of accountability measures to match the exponential increase in information sharing potential under the *SCISA*. The *SCISA* regime superimposes vast information sharing on top of existing imperfect information sharing structures already existent in Canada. Such a scheme may clarify for a hesitating, zealous official that they have a green light to now share information – but this scheme does absolutely nothing to ensure that reliability of information or constitutional principles are observed.

Information sharing in the national security context requires proper legal safeguards respecting necessity, proportionality, minimal impairment, and must comprise written agreements and caveats with respect to reliability, use, dissemination, access, retention and destruction. These safeguards are absent in the *SCISA* and the *Act* should be amended to rectify that.

In light of these essential safeguards, the only recipients of information sharing should be those agencies or departments with a mandate connected to the information being shared, and even then, information should only be shared if it meets checks regarding reliability, necessity and relevance. The reasons for listing agencies whose core duties do not relate to national security should be clearly stated.

In addition, there should also be safeguards in place to regulate the sharing of information between review bodies. In implementing the Arar Inquiry Policy Review's roadmap for ensuring effective review, as recommended further above, care must be taken to ensure that the review bodies receiving national security information have the required security clearances. Further, as the Commission noted, the recipient review bodies would need to have proper systems in place to preserve the security of information.[50]

---

[49] *Ibid*, *Charter* Application, at para. 34.
[50] Arar Inquiry, Policy Review, *supra* note 13, at 587-88.

4. The Passenger Protect Program

GREEN PAPER QUESTIONS

- *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?*

SECTION SUMMARY

The new *Secure Air Travel Act* ("*SATA*") gives the Passenger Protect Program ("PPP") its own legal basis and framework. In principle, this is positive and CCLA has long recommended a clear legislative basis for the program. Unfortunately, as currently codified, the *SATA* does not accomplish this goal. As we argue in our *Charter* challenge to the *ATA, 2015*, SATA unconstitutionally violates individuals' *Charter* rights to mobility and due process.

Moreover, even if the government's commitment to improving the redress process related to the PPP is effective and fixes the real problem of false positives to the list, these improvements are insufficient to address the PPP's violation of individuals' *Charter* rights.

SUBMISSION

CCLA's Charter Challenge

In its *Charter* challenge to the *ATA, 2015*, the CCLA maintains that SATA impairs the mobility interests of individuals placed on the no-fly list in violation of section 6 of the *Charter* and violates the liberty and security of the person interests protected by section 7 in a manner that does not accord with the principles of fundamental justice. These limits on individuals' mobility and due process rights are not reasonable or justifiable in a democratic society.

SATA codifies the power of the Minister of Public Safety and Emergency Preparedness to deny individuals air travel by placing them on a "no-fly list". Section 8 of the *SATA* authorizes the Minister to add anyone to the no-fly list on mere suspicion ("reasonable grounds to suspect") that he or she will "engage or attempt to engage in an act that would threaten transportation security" or will "travel by air for the purpose of committing an act of [terrorism]." Once placed on the no-fly list, it is very difficult for the individual to remove their name from the list. The *SATA* does not require the Minister to provide reasons to the individual for their no-fly designation.

As elaborated upon below, there is no due process, no fundamental justice, and no natural justice under this scheme.

The Secure Air Travel Act is unconstitutional and requires several reforms beyond the potential improvements discussed in the Green Paper

SATA codifies the power of the Minister of Public Safety and Emergency Preparedness to deny individuals air travel by placing them on a "no-fly list". Section 8 of the *SATA* authorizes the Minister to add anyone to the no-fly list on mere suspicion ("reasonable grounds to suspect") that he or she will "engage or attempt to engage in an act that would threaten transportation security" or will "travel by air for the purpose of committing an act of [terrorism]." Once placed on the no-fly list, it is very difficult for the individual to remove their name from the list. There is no due process, no fundamental justice, and no natural justice under this scheme. The *SATA* does not require the Minister to provide reasons to the individual for their no-fly designation.

While the CCLA agrees with the Green Paper suggestion of removing individuals from the list if a Minister fails to make a decision on an application for removal from the list, and with the government commitment to improving the redress process, these two procedural improvements will be ineffectual without a more complete overhaul of the listing process.

The CCLA has identified several major deficiencies of the *SATA* that would be unaddressed or inadequately addressed by the improvements to the program discussed in the Green Paper.

First, pursuant to the Act, the Minister may establish a list of persons who the Minister has reasonable grounds to suspect will "engage or attempt to engage in an act that would threaten transportation security" or "travel by air for the purpose of committing an act or omission that" is considered to be a terrorism offence under the *Criminal Code*. The Act gives no indication of how the Minister might form such a reasonable suspicion and the standard of reasonable suspicion is a low one given that the effect of listing could be a near-total abrogation of mobility rights guaranteed under s. 6 of the *Charter.*

The lack of certainty on how these listing decisions are made has been an ongoing problem in the implementation of Canada's air travel security. The OPC identified this concern in its 2009 Audit Report of the Passenger Protect Program, stating that the Minister (of Transportation) was not provided with complete information when deciding to add or remove names to or from the Specified Persons List, and that this posed serious consequences to the livelihood, reputation and ability to travel of the person named.[51] This concern raised by the OPC was not addressed in the Act. In fact, this problem was deepened by the inclusion of the Minister's authority – under s. 7 of *SATA* – to delegate his or her power, duties and functions under the Act to *any* officer or employee, or *any* class of officers or employees, in the Department of Public Safety and Emergency Preparedness. The authority to delegate can exacerbate the problem of relying on insufficient information in order to make listing decisions. The delegation also substantially dilutes (and can even eliminate) any meaningful accountability for the listing process.

Second, a person who has been denied transportation as a result of a Ministerial direction may apply to the Minister, in writing, to have their name removed from the list. This may only be done within sixty days of being denied transportation, although provisions of the *Act* do not make it clear how an individual may come to know that they have been listed, or that this will be done at the time that transportation is denied. Indeed, the *Act* suggests that a person who is denied transportation may not be informed of the fact that they have been placed on the list.[52] Section 20(3) of the *Act* prohibits air carriers from disclosing any information related to a listed person, including whether

[51] Office of the Privacy Commissioner of Canada, *Audit of Passenger Protect Program, Transport Canada* (17 November 2009), at para. 84, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_ppp_200910/>.
[52] *SATA, supra* note 22, s. 20(1).

or not an individual is listed. While individuals may, at present, be apprised of their status as a listed person via a written direction from Public Safety, there is still no assurance – statutory or otherwise – that all individuals will be so notified or that notification is effectively and promptly communicated.

An appeal mechanism is futile if the supposed beneficiary may have no way of knowing there is anything to appeal. Moreover, providing a listed person with a way to challenge their listing is useless if the inclusion of their name on the list is not effectively and promptly communicated.

Third, the appeals mechanism afforded by s. 16 of the *Act* allows the judge presiding over an appeal to hear information or evidence in the absence of the public and the appellant or his/her counsel. Although section 16(6)(c) purports to offer a procedural protection for the appellant in providing that "the judge must ensure that the appellant is provided with a summary of information and other evidence that enables them to be reasonably informed of the Minister's case," this protection is directly undermined by subsection 16(6)(f), which allows the judge to base a decision on the Minister's information or evidence, even if a summary has not been provided to the appellant. The ability for a judge to both use and rely on "secret evidence" is inconsistent with an overarching principle of fundamental justice: that the listed person/appellant has the right to know the case against her or him, and has the right to fully and fairly answer that case. The Supreme Court of Canada has held in another context that:

> As a general rule, a fair hearing must include an opportunity for the parties to know the opposing party's case so that they may address evidence prejudicial to their case and bring evidence to prove their position…The exclusion of the appellant from portions of the government's submissions is an exceptional departure from this general rule. The appellant operates in an informational deficit when trying to challenge the legitimacy of the exemptions claimed by the government."[53]

Despite s. 16(6)(d)'s assertion that "the judge must provide the appellant and the Minister with an opportunity to be heard," this right will not be meaningful if the appellant is unaware of the evidence against him/her.

Fourth, in light of the potential for the use of secret evidence in these appeals, we are concerned about the absence of a special advocate, a safeguard put in place in the security certificate regime under the *IRPA,* where secret evidence may also be used. Without a special advocate privy to the evidence and information submitted by the Minister, the listed person is at a significant disadvantage. In these circumstances, judicial oversight is insufficient to ensure that due process rights are respected. The government is represented at all times and apprised of all of the facts and allegations, while the listed person may be denied information crucial to the case against him/her. This creates an obvious imbalance of power. No matter how fair, able, and apprised of the facts the judge may be, the imbalance threatens the fairness and efficacy of the hearing. It also requires judges to simultaneously act as advocate and neutral arbiter, eroding the separation of functions which lies at the heart of the adversarial system. In CCLA's view, where secret evidence is used in these appeals, the appointment of a special advocate should be mandatory.

Fifth, section 16(5) of the *Act* states that if the judge finds that the decision denying removal from the list is unreasonable, the judge "may order that the appellant's name be removed from the list." It is unclear why the wording of the provision is discretionary (may) rather than mandatory (shall).

[53] *Ruby v. Canada (Solicitor General)*, 2002 SCC 75, [2002] 4 SCR 3 at para. 40.

If a decision to keep an applicant's name on the list is found to be unreasonable, the name should presumptively be removed.

Finally, the OPC's Audit Report from 2009 highlighted a number of privacy concerns, including issues around inadequate verification of the handling and safeguarding of listing information by air carriers. This issue, among others highlighted by the OPC, were not addressed in the *Secure Air Travel Act.* We recommend an overhaul of the *Secure Air Travel Act* that addresses the privacy recommendations in the OPC's Audit Report.

While a statutory requirement of removing individuals from the list in the event of Ministerial delay is an improvement over the current system, it would do little to ameliorate these constitutional failings of the current scheme. A more holistic overhaul of *SATA* is required in order to the protect individuals' *Charter* rights to due process and mobility of the person.

5. *Criminal Code* Terrorism Measures

GREEN PAPER QUESTIONS:

- *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?*

SECTION SUMMARY

The amendments to the *Criminal Code* introduced by the *ATA, 2015* were significant and unnecessary. The offence of promoting or advocating terrorism offences in general is not needed, given the already wide range of criminal terrorism offences. As we argue in our *Charter* challenge to the *ATA, 2015*, the offence is unconstitutional. It is overly broad and will chill legitimate dissent.

The new terrorist propaganda provisions give rise to similar concerns of vagueness, overbreadth, and unjustified restrictions of free expression. These new *Criminal Code* provisions make terror suspects harder to detect and investigate. Further, the lower thresholds for preventive arrest, detention and recognizances with conditions – already exceptional broad powers – are now amplified and undermine due process rights and the rule of law.

SUBMISSION

CCLA's Charter Challenge

In its *Charter* challenge to the *ATA, 2015*, the CCLA has maintained that the new speech offence of promoting or advocating terrorism offences in general is unconstitutional.

Freedom of expression includes not only the right to speak, write and express oneself, but also the rights of individuals in Canada to hear, read and listen. The censorship provisions have a chilling

effect on freedom of expression and will result in censorship and the seizure or deletion of content that may pose no genuine threat to Canada's safety.

Moreover, the phrase "terrorism offences in general" in the new speech offence is not defined in the *Criminal* Code and is unconstitutionally vague and imprecise. The new speech offence does not provide fair notice to citizens of the consequence of their speech or conduct, nor or does it sufficiently limit state agents charged with enforcing the provision. As such, the prohibited speech and conduct are neither fixed nor knowable by citizens in advance.

Consequently, and for reasons elaborated upon below, the new speech offence is an unconstitutional infringement of individuals' section 2 and section 7 rights to freedom of expression and due process.

The Criminal Code Amendments Were Unnecessary and Should Be Repealed

The *ATA, 2015* amended the *Criminal Code* to create a new offence of advocating or promoting the commission of terrorism offences in general, to provide new powers to address terrorist propaganda and to lower thresholds for preventive arrest, recognizance orders, and for peace bonds. The creation of new offences and powers suggested that our previous criminal provisions were inadequate and needed to be enhanced. However, this case was not and has not been effectively made. There is still no evidence that the offences and criminal law powers introduced by *ATA* are necessary or that they have been or will be effective. In some cases, the evidence indicates that the new offences may undermine safety and security by driving those who express extremist ideas in quasi-public forums further underground. This form of expression can be a valuable tool for intelligence and law enforcement agencies.

The offence of advocating and promoting the commissions of terrorism offences is unnecessary and unconstitutional

The new offence against advocating or promoting terrorism offences in general states:

> 83.221(1) Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general – other than an offence under this section – while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.

This is a speech crime. It criminalizes the expression of ideas and therefore engages core constitutional protections for freedom of expression and freedom of the press. Freedom of expression is a fundamental freedom – and a bedrock right in a democracy. The creation of criminal offences directed purely at expressive activity must be subject to careful scrutiny in any democratic system that values the free exchange of ideas. Robust protection for freedom of expression does not deny that expression can be harmful, but recognizes the value in countering and denouncing such expression rather than resorting to state-sponsored censorship.

The speech offence is both exceptionally broad and vague. The provision criminalizes advocacy or promotion of "terrorism offences in general" – a reference to a concept that is not defined in the *Criminal Code* and extends beyond the defined terms of "terrorist offence" or "terrorist activity" (both of which are already expansive).[54] The breadth of this term stands in contrast to narrowly

[54] See *Criminal Code, supra* note 21, ss. 2, 83.01(1).

defined terms that lie at the heart of other expression-based offences including the willful promotion of hatred and the child pornography offences.[55] It captures statements that are made privately, intruding into personal relationships in a way that is simply not justified, and may, for reasons explored further below, undermine ongoing counter-radicalization efforts. The breadth of the offence is extended even further since aiding and abetting the offence is also a basis for criminal liability. The provision requires that the accused "knowingly" advocate or promote "terrorism offences in general" thus setting a lower *mens rea* standard than the more demanding "willful" language used in association with hate speech provisions. Further, the new offence contains no specific defences. It is difficult to conceive of an expression-based offence that captures more.

In CCLA's view, the offence is overbroad, vague, and cannot withstand constitutional scrutiny. Moreover, the government has not demonstrated any compelling reason why such an offence is necessary.

The government Green Paper has argued that the new offence was required to cover the criminal counselling of terrorism offences when counselling is not specific as regards the offence or type of offence. This is not a credible justification for the new offence.

The *Criminal Code* already contains a large number of offences that address terrorism in a variety of different forms. The existing provisions include financing offences, (83.02-83.04), and participating, facilitating, instructing and harbouring offences (ss. 83.18-83.23). In addition, the *Criminal Code* defines "terrorism offence" in part as including *any* indictable offence committed for the benefit of, at the direction of or in association with a terrorist group. It also extends to a conspiracy, attempts to commit, being an accessory after the fact, or any counselling in relation to a terrorism offence. These offences already catch a great deal of behavior that involves no violence and that may have only a very remote connection to what most Canadians would consider an act of terror.

In light of the restriction the offence places on free expression, the government must demonstrate why it is justified. To date, the government has not shown how this provision will assist in the fight against violent extremism, which is already well-addressed in our *Criminal Code*.

CCLA has a number of concerns about the impact that the offence may have on Canadians, regardless of whether it is actually used to prosecute individuals. The mere existence of this offence "on the books" has the potential to chill or stifle freedom of expression and freedom of the press in a manner that is neither reasonable nor demonstrably justified.

Given the breadth of the terrorism offences, and the addition of the phrase "in general" in the offence, it is not only those who advocate or promote suicide bombings or mass shootings that could be caught within the law's ambit. Individuals speaking out about foreign wars and expressing their views about who is on the "right side" risk being caught by the law. Individuals who wish to encourage financial assistance to humanitarian organizations that have some tenuous or suspected links to listed terrorist entities (including entities that may control territory or act as the *de facto* government in a region) would also fall under the law's large umbrella. The freedom of journalists is put at risk and academic freedom suffers. The chill that this law has had, and could have, on expressive freedom cannot be known or measurable, since those with controversial and unpopular views will simply not express themselves.

[55] See e.g. *R. v. Keegstra,* [1990] 3 S.C.R. 697, 77 Alta LR (2d) 193, and *R. v. Sharpe,* 2001 SCC 2, [2001] 1 SCR 45.

In addition to the chill that this law can cast on legitimate expression on matters of public interest, it can also hinder the ability of law enforcement and intelligence agencies to meaningfully monitor threats and investigate useful leads.

Further, counter-radicalization efforts can be undermined. Free speech can be an important tool in fighting radicalization and promoting free exchange of ideas. Intervention in the early stages of radicalization will require frank discussions about an individual's views on controversial topics. If these individuals can be charged for the simple (and private) expression of their views, the already difficult task of de-radicalization will be rendered all the more challenging.

The provisions on seizure and deletion of "terrorist propaganda" should also be repealed

The new terrorist propaganda provisions, contained in ss. 83.222 and 83.223 of the *Criminal Code,* created new powers to allow for the seizure or deletion of "terrorist propaganda", defined as "any writing, sign, visible representation or audio recording that advocates or promotes the commission of terrorism offences in general – other than an offence under subsection 83.221(1) – or counsel the commission of a terrorism offence." These powers give rise to concerns of vagueness, overbreadth, and unjustified restrictions of free expression that are similar to those outlined above. By lumping in the advocacy or promotion of "terrorism offences in general", this law can sweep up a wide range of material that may have little to do with genuine terrorist threats. Freedom of expression is not just significant for the speaker or author, but also for the listener or reader. Allowing for deletion of materials that may be harmless (and might even help in provoking meaningful debates and discussions on matters of public interest) affects the rights of Canadians not just to speak, but also to hear.

The propaganda provisions allow for the owner, author or person who posted the material to come forward and participate in the hearing on the issue of seizure or deletion. While this is an important safeguard, its utility is significantly undermined given the existence of the promotion/advocacy offence. An individual would have good reason to be concerned about whether coming forward could expose them to criminal liability. As a result, any judicial considerations of the terrorist propaganda powers may well occur without the benefit of an adversarial hearing.

There are three further concerns with the terrorist propaganda provisions that merit attention. First, it is likely that law enforcement or intelligence services are able to easily avoid the judicial process by simply approaching internet service providers or companies that host content and ask for voluntary removal.[56] Given that, under the law's broad remit these companies can themselves be liable for hosting this content, cooperation is likely. Even if we accept that removing this content from the Internet is an appropriate and constitutionally-compliant tactic, circumventing the judicial process (and the law's requirement for the consent of the Attorney General before seeking a seizure or deletion order) creates a private censorship scheme without meaningful review. A society that takes freedom of expression seriously should reject such an approach.

Second, Professors Roach and Forcese have pointed to the concerns about the incorporation of "terrorist propaganda" into the material that can be stopped at the border by customs officials. The breadth of material that can be caught under this is, as outlined above, troubling in any context, but particularly so when applied by border officials with minimal relevant training and with no body dedicated to review.

---

[56] See Craig Forcese & Kent Roach, *Bill C-51 Backgrounder #4: The Terrorism Propaganda Provisions* (23 February 2015) at 20, online: SSRN <http://ssrn.com/abstract=2568611>.

Finally, both the speech offence and the terrorist propaganda provisions can negatively impact Canada's ability to engage in counter-radicalization activities. CCLA's position on freedom of expression has long been that offensive or hateful expression should be denounced and countered, not censored. While the issue of radicalization is a complex one that lies beyond the scope of our primary expertise, we are troubled that the *ATA* took an approach to radicalization that is narrowly focused on the criminal law and that did not address the need for educational and outreach strategies to counter radical messages that may be persuading some individuals to take violent action in or against Canada. This lopsided approach suggests that rather than seeking to balance and reconcile freedom and security, the provisions introduced by the *ATA* have the potential to undermine both.

The thresholds for preventive arrest, recognizance and peace bonds are unnecessary and inappropriate

Another significant change created by the *ATA, 2015* was new *Criminal Code* sections regarding preventive arrest, recognizances and peace bonds. The preventive arrest and recognizance measures were originally part of a package of changes made to the *Code* in the *Anti-terrorism Act, 2001*.[57] The exceptional provisions were subject to a sunset clause, had not been used, but were reintroduced in 2012 despite widespread criticism and concern expressed by civil society groups. In particular, at the time that these controversial measures were re-introduced, CCLA and a number of other rights organizations issued a statement expressing our strong disagreement, stating in part:

> Renewing these provisions would normalize exceptional powers inconsistent with established democratic principles and threaten hard-won civil liberties. Commitment to the rule of means that counter-terrorism measures must adhere to the values embodied in the *Charter of Rights and Freedoms,* and cannot infringe on basic rights.[58]

These exceptional powers allowing for detention and for the imposition of conditions on individuals absent any charge have been re-enacted in the *Code* despite the fact that they were not necessary (or employed) to thwart multiple terrorist plans. Moreover, even before the terrorism provisions were introduced, the *Code* already allowed for detention of an individual where an officer has reasonable grounds to believe the individual is "about to commit an indictable offence"[59]. The *Code* also imposes criminal liability for a number of inchoate offences, including attempts and conspiracies. Individuals charged with these crimes can be detained without bail in appropriate circumstances, or released on conditions. In sum, the special terrorism provisions for preventive arrest, peace bonds, recognizances and detention are not necessary and were not justified when they were re-enacted. The *ATA* then lowered the evidentiary thresholds that must be met before these measures can be imposed. This demonstrates how easily exceptional measures once considered necessary for a limited purpose and period of time can become integrated into the ordinary criminal law. The absence of any sunset clauses confirms that preventive arrest is no longer considered extraordinary or unusual in our system.

In addition to the question of need, CCLA is also concerned about the efficacy and impact of the new thresholds. The standards are so loose that they would appear to allow these exceptional measures to be applied in a wide variety of cases that may not present any genuine danger or significant

---

[57] *Anti-terrorism Act,* S.C. 2001, c. 41.

[58] Canadian Civil Liberties Association, *Statement on Reintroduction of Anti-Terrorism Provisions* (28 November 2012), online: CCLA <https://ccla.org/cclanewsite/wp-content/uploads/2015/03/20121128-Statement-on-Reintroduction-of-Anti-Terrorism-Provisions.pdf>.

[59] *Criminal Code, supra* note 21, s. 495.

threat to public safety. Officers may lay an information where they believe on reasonable grounds that a terrorist activity (defined broadly) may be carried out or where they suspect on reasonable grounds that the imposition of a recognizance with conditions on a person, or the arrest of a person, is likely to prevent the carrying out of a terrorist activity. These standards can result in detention in custody for a period of up to seven days and the imposition of a recognizance with conditions for up to a year (or more if the judge is satisfied that the individual was previously convicted of a terrorism offence).

The *ATA* also created a new peace bond provision in the *Criminal Code* allowing a person who "fears on reasonable grounds that another person may commit a terrorism offence" to lay an information with the Attorney General's consent. Where a judge is satisfied that the informant has reasonable grounds for the fear, a recognizance of up to twelve months may be imposed (a five year period is permitted where the judge is satisfied the defendant was previously convicted of a terrorism offence). The conditions that may be imposed with the recognizance are wide-ranging and can be intrusive and extremely restrictive, including weapons prohibitions, surrender of passport and more general restrictions on mobility. The punishment for breaching conditions has also been increased, even though the conditions may have little or no connection to the allegedly dangerous activity the individual is suspected of planning. The judge may commit the individual to prison for up to twelve months if he/she fails or refuses to enter into the peace bond.

These are exceptional incursions into liberty and are based on watered down standards that do not provide meaningful guidance to law enforcement or judges. It is well-accepted that a liberal democracy does not eliminate or significantly restrict individual liberty absent a compelling reason (and usually a criminal charge). The lowering of standards to make this part of the *Code* easier to invoke is troubling and its necessity has not been established.

6. Investigative Capabilities in a Digital World

GREEN PAPER QUESTIONS

- *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?*

SECTION SUMMARY

CCLA is concerned that questions of expanding state surveillance and policing powers have been introduced into this consultation with insufficient context or public education on complex issues and unfamiliar technologies.

We believe that prior to increasing or changing investigative capabilities, Canadians need access to an evidence-based analysis of the actual risks to public safety from changing technologies, which must include an assessment of whether problems identified are potentially based in lack of training or resources. We need to consider not just what police would like, but what we, as a society, think is necessary and proportionate to legitimate risks.

Furthermore, CCLA respectfully submits that the challenge the Canadian government faces should be seen to be as much about regulating the use of intrusive new surveillance technology as it is about creating new kinds of access to Canadian's personal information via legislation. Investigative agencies should operate in the digital world as they are required to operate in the physical world: in accordance with law and with respect for our *Constitution* and our *Charter of Rights and Freedoms*.

The Green Paper discusses the following investigative tools in particular: lawful access to basic subscriber information without a warrant, mandated interception capabilities and retention requirements, and compelled decryption. CCLA presents reasons why all of these tools are problematic at best, and unconstitutional at worst.

Principles are not—and should not be--affected by platform. And regardless of the existence of a rich record of the activities most of us engage in daily that is facilitated by technology, most people do not expect that the state will, or should, have unhindered access to these records.

SUBMISSION

Overview

CCLA finds the tone and focus of the questions in this section to be highly problematic. They inherently suggest that changes are necessary and lead towards particular kinds of answers favorable to increased investigative powers. While we have addressed these questions in this submission, we would also like to raise the concern that the framing in the Green Paper may not have provided participants in this consultation with the fulsome understanding of the rights issues at stake in this discussion that they should have been given. The issues raised in the Green Paper about compelled decryption, warrantless access, and lawful access are complicated and fraught; the simple examples of ways that changes to laws might help police that are provided in the consultation background paper provide a very narrow perspective that fails to appropriately educate consultation participants on the risks to their rights. This section of the consultation goes beyond the scope of Bill C-51 and national security more generally, and conflates public safety, policing powers, and national security. These topics warrant separate, individual conversations and we caution that unlike the provisions of Bill C-51, which were extensively discussed and debated in the public sphere, the topics covered under investigative capabilities were not. The information deficit thus created will inevitably skew the findings of this consultation.

For evidence, we need look no further than to the shifting public perceptions of Bill C-51. When it was introduced in January 2015, 82% of people surveyed in an Angus Reid poll supported the legislation.[60] A few months later, after the specific provisions of the Bill were more widely known and the implications for Canadians and Canadian society had been more thoroughly discussed, support plummeted to around 33%.[61] The same is very likely to happen in the current discussion around fears of "going dark" and the expansion of police powers, once the benefits and risks of the

[60] Angus Reid Institute, *Bill C-51* (19 February 2015), online: <http://angusreid.org/wp-content/uploads/2015/02/2015.02.19-C51.pdf>.

[61] Forum Research, *Support for Bill C51 waning*, online: <http://poll.forumresearch.com/post/256/most-see-bill-having-negative-effect-on-their-lives>.

proposed expanded powers are more fully examined. If we consider a recent survey commissioned by the Toronto Star regarding many of the proposals for expanding policing powers discussed in the Green Paper, 77% of respondents said they thought police should be able to compel a password from a suspect to decrypt a cell phone or computer if they got a warrant to do so. However, 85% of same pool of respondents indicated that they had either never used encryption or weren't sure if they had.[62] This tells us two things: many people aren't entirely sure how encryption works or its value in the communication infrastructure, and they don't see how allowing police this power will affect them. The primary concern in relation to this proposed power of decryption is that it may compromise Canadian's *Charter*-protected right against self-incrimination; this significant potential for rights violations is glossed over in the Green Paper, and is clearly not yet part of the public conversation, and yet it is a fundamental problem with the proposal that Canadian's are being asked to evaluate.

CCLA cautions against drawing the conclusion that Canadian's support expanded state surveillance powers simply on the basis of a series of leading questions, with inadequate public education, on complex topics involving unfamiliar technologies.

Addressing challenges to law enforcement and national security investigations posed by the evolving technological landscape in a manner that is consistent with Canadian values

When it comes to policing and national security, far too often Canadians are asked to let fear trump their rights. The "going dark" metaphor that is central to this conversation in the popular press is a masterful public relations construction that frames the debate and encourages us to ask particular kinds of questions. If technology is leaving our police in the dark, shouldn't we do everything we can to turn on the light? The problem with this dramatic framing is that it often fails to withstand critical scrutiny. While it is true that some technologies may make an investigation more difficult, it is equally true that police have at their disposal a host of new technologies that facilitate investigations, including devices and techniques that permit mass surveillance (e.g. IMSI Catchers, colloquially known as Stingrays). And while it is true that changes to laws to make it easier to access private data without warrants, or to compel private sector companies to provide back doors and retain data would make the job of police easier, that is not necessarily the appropriate goal if we consider the public good. We have laws limiting police powers, and safeguards over these powers, because we, as a society, have decided that there are times when rights are so important that protecting them takes precedence.

Consider the technology that is increasingly presented in the media, or by public safety officials, or even in this consultation, as a danger: encryption. It is often characterized as a technology that prevents those whose job it is to keep us safe from fulfilling their role. However, in the vast majority of transactions online by ordinary, law-abiding citizens, encryption is a good thing that makes personal, sensitive data harder to capture and decipher. Indeed, if more data were stored in encrypted form, sensational breaches of privacy — like the one that drove some Ashley Madison users to suicide — could be avoided. Acknowledging that encryption can be a good thing for society doesn't erase police concerns about data access but it does provide very necessary contextualization.

Further, reports indicate that in many cases police now have the tools, and are working with technology companies, to gain access to even the most complex of encrypted data. For example, as

[62] Robert Cribb, Dave Seglins & Chelsea Gomez, "Canadians support police calls for more digital powers—with a catch: Toronto Star/CBC poll", *The Toronto Star* (17 November 2016) online: <https://www.thestar.com/news/canada/2016/11/17/canadians-support-police-calls-for-more-digital-powers-with-a-catch-toronto-starcbc-poll.html>.

we learned from the Project Clemenza investigation, police can now decrypt BlackBerry communications and are making extensive use of Stingray technology, which allows for the mass interception of cellphone data.[63] Even in the Apple vs. FBI case, the FBI managed to acquire the data they wanted without requiring Apple to compromise the security of every iPhone user in the world, despite the initial public statements that staked the success of an emotional case on a request for that drastic solution. In other words, the evolving technological landscape does not just pose challenges, it provides solutions.

We need evidence-based analysis of the actual risks to public safety from changing technologies, which must include an assessment of whether problems are based in lack of training or resources. We need to consider not just what police would like, but what we as a society think is necessary and proportionate to legitimate risk.

Furthermore, CCLA respectfully submits that the challenge the Canadian government faces should be seen to be as much about regulating the use of intrusive new surveillance technology as it is about creating new kinds of access to Canadian's personal information via legislation. As noted, police have access to powerful new surveillance technologies and techniques. Canadians have legitimate concerns that when a powerful technology is used in secret, it's impossible to ascertain whether it's being used wisely and proportionately, and if necessary safeguards are in place.

How should investigative agencies operate in the digital world?

Investigative agencies should operate in the digital world as they are required to operate in the physical world: in accordance with law and with respect for our *Constitution* and our *Charter of Rights and Freedoms*.

Principles are not—and should not be--affected by platform: if people have a reasonable expectation of privacy in a private conversation in Canada, that expectation should hold whether the conversation takes place in person, or by text message. If people have the right to free expression, that right is as relevant on a social media site as it is on a street corner.

One scenario in the Green Paper describes the fact that because police have inadequate evidence to acquire a warrant, they are denied access to basic subscriber information that would help them identify a suspect at the beginning of an investigation.[64] This is presented as a profound problem for law enforcement. But CCLA would argue that we have warrant requirements precisely to ensure that an individual's privacy is not invaded without sufficient cause. To us, this scenario suggests that our current law, as it has been interpreted following the case *R v. Spencer*, is working exactly the way it should to protect Canadians' section 8 rights against unreasonable search and seizure.

We would like to reiterate here the statement we made in our submission to the CyberSecurity Consultation in October 2016: The CCLA believes that it is eminently possible to protect rights and public safety at the same time. However, this requires rights to be considered not as a barrier or a necessary evil to be worked around in policy and practice, but rather as a fundamental component of genuine safety. Furthermore, in a time when individuals increasingly lack control over information they create, or that others create about them, they need to know that the law enforcement agencies charged with keeping them safe are not themselves unnecessarily or disproportionately capitalising on this loss of control.

---

[63] See Dave Seglins & Matthew Braga, "RCMP can spy on your cellphone, court records reveal," *CBC News* (11 June 2016) online: <http://www.cbc.ca/news/technology/rcmp-blackberry-hack-montreal-mob-murder-pub-ban-lifted-1.3629222>.

[64] Green Paper, *supra* note **Error! Bookmark not defined.**, at 57.

Should the Government update investigative tools to better support digital/online investigations?

The Green Paper discusses the following investigative tools in particular: lawful access to basic subscriber information without a warrant, mandated interception capabilities and retention requirements, and compelled decryption.

CCLA argues against the Green Paper's reintroduction of "lawful access," an issue previously settled by the Supreme Court of Canada ("SCC") in *R v. Spencer,* which held that a warrant is required as a matter of balancing investigative needs against *Charter* rights in cases where a name and address linked to an IP address would reveal intimate details about online activities. Rights-protecting thresholds in the investigatory process, such as evidentiary thresholds, should be upheld, not eroded.

CCLA argues against mandating private sector companies to build interception capabilities into their systems, as it renders them more vulnerable in the name of security. Neither do we support forcing private sector companies to retain information longer than necessary for business purposes, which again serves to undermine security, increase the risk of breaches and create more attractive targets for malicious attacks. We would note in the context of data retention that in 2014 the European Court of Justice, in a landmark judgment, struck down the EU's "Data Retention Directive" because it was in breach of the *Charter of Fundamental Rights of the European Union*. Similar indiscriminate retention of every Canadian's data would very likely violate our own *Charter of Rights and Freedoms*.

CCLA is against compelled decryption. In our view, the creation of a power to compel decryption would almost certainly be considered unconstitutional in Canada. The right not to be conscripted against oneself, as well as the protection against self-incrimination, are enshrined in the *Canadian Charter of Rights and Freedoms* ss. 11(c) and 13, and are fundamental organizing principles of the criminal law. Moreover, critical privacy rights are at stake when police seek to interfere with electronic devices. This cannot be taken lightly. We note that testimonial evidence, such as a password, is not the same as physical evidence such as that collected in breathalyzers or DNA tests. And further, while we are supportive of the warrant process in most situations, asking judges to issue warrants to circumvent a constitutional protection is not the same as asking them to weigh a potential infringement against a social benefit.

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

The fact that data is often tracked and stored by the private sector when we interact online, and the fact that conversations are recorded and not ephemeral, does affect expectations of privacy. In some cases, people respond to this by using privacy protective technologies. In other cases, they throw up their hands in despair and do nothing. And sometimes, they make choices about what technologies they use when, and for what purposes.

But regardless of individual's responses to the privacy dilemmas created in the online world, and regardless of the existence of a rich record of the activities most of us engage in daily that is facilitated by technology, most people do not expect that the state will, or should, have unhindered access to these records. The fact that police or intelligence agencies want greater abilities to retroactively seize or intercept records of private activities created during the course of daily life does not mean that this access should be considered necessary or even desirable in a society that values freedom and the presumption of innocence.

Expectations of privacy are normative and they are not based on the affordances of technologies but on our perceptions of the rights and freedoms we should enjoy in a democratic state subject to rule of law. Canadians expect the ability to live lives without state intrusion; exceptions in the digital world must be, as they have always been in the physical world, subject to careful scrutiny and evaluated in terms of necessity and proportionality.

7. Intelligence and Evidence

GREEN PAPER QUESTIONS

- *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?*

SECTION SUMMARY

In our *Charter* Challenge, CCLA submits that in particular, the amendments under sections 83(1) and 85.4(1) which permit the Minister of Public Safety and Emergency Preparedness to withhold information from special advocates appointed to protect the rights of individuals subject to security certificates violate section 7 of the *Charter*.

In general, the CCLA is seriously concerned that the lessons regarding intelligence and evidence identified by the Air India Commission of Inquiry are absent from the *ATA, 2015* and indeed the Green Paper. CCLA reiterates the need for greater accountability measures in national security policies and practices. Increased accountability, through independent, security-cleared bodies, could improve the protection and use of national security information in criminal, civil and administrative proceedings, while respecting individuals' rights and freedoms.

CCLA recommends expanding the vital role of security-cleared lawyers like special advocates beyond the security certificate context to all types of proceedings where the person is not allowed to know the extent of the proceeding before them, including proceedings under section 38 of the *Canada Evidence Act*.

Unfortunately, amendments to the *IRPA* under the *ATA, 2015* backpedal on these and other important protections in the security certificate regime.

SUBMISSION

CCLA's Charter Challenge

In our Challenge, CCLA notes that Part 5 of the *ATA, 2015* amends the Immigration and Refugee Protection Act ("IRPA") to permit the Minister of Public Safety and Emergency Preparedness, under sections 83(1) and 85.4(1) of the IRPA, to withhold information, including information relevant to the government's case in a security certificate proceeding, from the special advocate appointed to protect the interests of the individual who is the subject of the proceeding. Prior to the amendment, special advocates received all information in the government's possession relating to the individual's case. These amendments violate section 7 of the *Charter* by imperilling the life, liberty and security of the person interests of the individual in a manner that does not accord with the principles of fundamental justice; and the amendments prevent the special advocates from serving their constitutionally required roles in accordance with the Supreme Court of Canada's holdings in the cases of *Charkaoui v. Canada (Citizenship and Immigration)*, [2007] 1 SCR 350 and *Canada (Citizenship and Immigration) v. Harkat*, [2014] 2 SCR 33.

Canada Evidence Act, section 38 does not properly balance fairness and security

The current section 38 procedures of the *Canada Evidence Act*[65] do not properly balance fairness with security in legal proceedings. Under section 38, a judge of the Federal Court assesses whether disclosure of national security information would be injurious and, if so, must rule on the disclosure that balances the public interest in disclosure and non-disclosure. This determination is always made by a Federal Court judge, even in proceedings before a different court.

The existing checks are insufficient to balance the unfairness caused by the current section 38 system. The Air India Commission of Inquiry highlighted "real and serious" problems with section 38.[66] First, as established in the Supreme Court's decision in *Harkat*, the judge is supposed to play a "gatekeeper" function, ensuring a fair process and that the record supports the non-disclosure of the information.[67] But in a proceeding before a different court, a Federal Court judge lacks the contextual knowledge of the trial judge, which is essential to an informed ruling. Second, under section 38.14, the trial judge in a criminal proceeding also bears the burden of ensuring a fair trial, but must do so without knowing the secret information that was not disclosed.[68] The trial judge also has remedial powers under section 24(1) of the *Charter*; however, because of the section 38 jurisdictional bifurcation, the trial judge lacks the power to order that the Federal Court's non-disclosure ruling be revised, should new facts come to light.[69]

The Commission's final report also included testimony from witnesses before the Commission attesting to the inefficiency of the bifurcated proceedings. Former CSIS and RCMP officials attributed the system to trial delays and called for change.[70]

---

[65] *Canada Evidence Act*, R.S.C. 1985, c. C-5, s. 38.
[66] Air India Inquiry, Final Report, *supra* note 17, s. 7.3, at 160.
[67] *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37, [2014] 2 SCR 33, at para. 46 [*Harkat*], citing Craig Forcese & Lorne Waldman, *Seeking Justice in an Unfair Process: Lessons from Canada, the United Kingdom, and New Zealand on the Use of 'Special Advocates' in National Security Proceedings* (1 August 2007), at 60, online: SSRN <http://dx.doi.org/10.2139/ssrn.1623509>.
[68] *Canada Evidence Act*, *supra* note 65, s. 38.14(1). See also Air India Inquiry, Final Report, *supra* note 17, s. 7.3, at 160.
[69] *Ibid*, Air India Inquiry, Final Report.
[70] *Ibid*, s. 7.2.5, at 158.

Although the Supreme Court of Canada found that the bifurcated section 38 procedure applied in criminal cases survived constitutional scrutiny,[71] in the *R. v. Ahmad* decision the Court noted that the question in issue was not whether the section 38 bifurcation is "unusual [. . .] undesirable [. . .] or inefficient", and left it open to the government to evaluate whether the system should be changed.[72]

The Commission stated that the section 38 bifurcated system has "serious and irremediable disadvantages" and that it was "not likely" that the system could be saved.[73] The Commission concluded that,

> The present two-court system used in deciding section 38 applications is out of step with systems in other democracies. The two-court structure has demonstrated unequivocally that it is a failure.[74]

Improve section 38: Abandon the bifurcated system and adopt the special advocate program

To improve the existing section 38 procedures, the government should reconsider the recommendations from the Air India Commission of Inquiry. The Commission recommended discontinuing the use of the bifurcated system for section 38 claims in criminal cases. The Commission suggested amending section 38 to empower the criminal trial court and its judges to rule on disclosure of national security information in such cases.[75] This would be consistent with the procedure in Australia, the United Kingdom and the United States, where the trial judge has the power to review the confidential information and decide on its disclosure.[76] The Commission also recommended expanding the *IRPA* special advocate program to proceedings under section 38 of the *Canada Evidence Act*.[77]

Implementing these improvements would allow disclosure decisions to be fully informed by the facts and context of the case before the trial judge in criminal cases, and would assist the judge in ensuring trial fairness. The special advocates, with their top-level security clearance, would help maintain confidentiality of the information from the accused and their counsel and ensure procedural fairness by arguing for the accused's access to information that is relevant to the case.

Non-legislative measures: Greater accountability is needed

With respect to non-legislative measures which could improve both the use and protection of national security information in criminal, civil and administrative proceedings while respecting the principles of fundamental justice, CCLA reiterates the need for greater accountability measures in national security policies and practices. For example, the Air India Inquiry's first recommendation was the enhancement of the National Security Advisor in the Privy Council Office to supervise and oversee all national security initiatives of the various government agencies.[78]

Accountability policies need to be formulated with a view to the fact that the confidential nature of national security activities makes it more difficult to rely on customary public checks on

---

[71] *R. v. Ahmad*, 2011 SCC 6, [2011] 1 SCR 110 at paras. 81 [*R. v. Ahmad*].
[72] *Ibid*, at paras. 5, 80.
[73] Air India Inquiry, Final Report, *supra* note 17, s. 7.3, at 160, 163.
[74] *Ibid*, s. 7.3, at 160.
[75] *Ibid*, s. 7.4, Recommendation 19, at 165.
[76] *Ibid*, s. 7.2.4, at 157, citing Kent Roach, "The Unique Challenges of Terrorism Prosecutions: Towards a Workable Relation Between Intelligence and Evidence" in *Research Studies: The Unique Challenges of Terrorism Prosecutions*, vol. 4, at 286.
[77] *Ibid*, s. 7.6, Recommendation 21, at 169.
[78] *Ibid*, s. 2.3.3.11, Recommendation 1, at 47, 333.

government bodies. Having independent, security-cleared review and oversight bodies in place is essential to achieving a balance between protecting national security while respecting individuals' rights and freedoms.

The important role of security-cleared lawyers

CCLA's position is that security-cleared lawyers in legal proceedings where national security information is involved have the essential role of protecting the interests of affected persons in closed proceedings, while ensuring that confidential national security information is not fully disclosed to those persons.

CCLA strongly supports the use of the special advocate program created by Parliament to provide some procedural protections to those subject to security certificates. Special advocates are allowed access to secret evidence, without fully disclosing the case to named persons. With access to the secret evidence, the special advocates can test and challenge the evidence *in camera* on behalf of the named individuals. The program was implemented in the security certificate context in response to the Supreme Court of Canada's clear interpretation of section 7 rights in *Charkaoui v. Canada (Citizenship and Immigration).*[79] In that case, the Court found that, prior to the existence of the special advocate system, the procedure for judicial approval of security certificates was unconstitutional, as the rights of the named person to know the case against him/her and challenge it, were denied due to secrecy in the proceedings. In a unanimous decision, the Court found that inability to know the case against him/her violated principles of fundamental justice. The Court stated that the informed scrutiny, challenge and opposing evidence of a person who is familiar with a case, such as counsel or a special advocate, is "the whole point of the principle that a person whose liberty is in jeopardy must know the case to meet."[80] The Court further stated that the national security context cannot be used to "erode the essence"[81] of the section 7 protection which is meant to provide "meaningful and substantial protection"[82] and due process.

The role of security-cleared lawyers like special advocates was outlined by the Air India Commission of Inquiry. In recommending that the special advocate program be adopted under section 38 of the *Canada Evidence Act*, the Commission submitted that legal proceedings with only one side present may be unfair if the judge is accustomed to an adversarial setting. The Commission submitted that the expansion of the special advocate role to proceedings beyond the security certificate context would assist the court in balancing disclosure and protecting national security.[83]

Expand the special advocate program to all types of proceedings to balance protection of information with respect for the principles of fundamental justice

CCLA recommends that the role of special advocates should be expanded beyond the security certificate context to all types of proceedings, whether criminal, civil or administrative, to improve the protection of national security information while ensuring a balance with the principles of fundamental justice.

The Air India Commission of Inquiry was right in recommending the extension of special advocates to section 38 *Canada Evidence Act* proceedings, discussed above.[84] The special advocate program

---

[79] *Charkaoui v. Canada (Citizenship and Immigration)*, 2007 SCC 9, [2007] 1 SCR 350 [*Charkaoui*].
[80] *Ibid,* at para. 64.
[81] *Ibid,* at para. 27.
[82] *Ibid.*
[83] Air India Inquiry, Final Report, *supra* note 17, s. 7.6, at 168.
[84] *Ibid*, s. 7.6, at 168.

should not be confined to the security certificate context; it should be used in *any* proceeding where a person is not allowed to know the extent of the proceeding before them, whether that be a criminal, civil or administrative proceeding, as much as doing so is practical. The increased use of special advocates would better facilitate balancing the public interest in disclosure of the information and due process with the public interest in national security.

The IRPA changes reverse section 7 protections in the security certificate regime and are not balanced by safeguards in place

Unfortunately, far from expanding the special advocates program, the *ATA, 2015* frustrates the program with its regressive changes to the *IRPA*, Division 9, relating to security certificates. This is CCLA's chief concern among the questions posed in the Intelligence and Evidence section of the Background Document. It is CCLA's position that the changes to the *IRPA* cannot be appropriately balanced by safeguards.

In particular, CCLA is concerned that sections 83(1) (as amended by *ATA, 2015,* section 57) and 85.4(1) (as enacted by section 59 of the *ATA, 2015*) of the *IRPA* allow the Minister to withhold information from a special advocate, including information relevant to the government's case in a security certificate proceeding.

These amendments are unconstitutional. CCLA, along with Canadian Journalists for Free Expression ("CJFE"), is challenging sections 57 and 59 of the *ATA, 2015*, claiming that these amendments to the *IRPA* violate section 7 of the *Charter* in a manner that cannot be saved by section 1.[85] Sections 83(1) and 85.4(1) of the *IRPA* permit the Minister of Public Safety and Emergency Preparedness to withhold information, including information relevant to the government's case in a security certificate proceeding, from a special advocate appointed to protect the interests of the individual who is the subject of the proceeding. Prior to the amendment, special advocates received all information in the government's possession relating to the individual's case.[86] The purpose of the section 7 liberty protection is for the person whose liberty is in jeopardy to know the case to be met and to allow them to make full answer and defence. As such, these amendments violate section 7 of the *Charter* by imperilling the life, liberty and security of the person interests of the individual in a manner that does not accord with the principles of fundamental justice. These violations do not constitute reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society under section 1 of the *Charter*.[87]

They also violate the Supreme Court of Canada rulings in *Charkaoui*[88] and *Canada (Citizenship and Immigration) v. Harkat*,[89] regarding the interpretation and meanings of the section 7 protection. In particular, these changes fly in the face of the Supreme Court of Canada's statement in *Charkaoui,* noted above, that the national security context cannot be used to "erode the essence" of the section 7 protection, which is meant to provide "meaningful and substantial protection" and due process.[90]

These changes are not appropriately balanced by the safeguards in place. In fact, these changes, upend the post-*Charkaoui* protections in the *IRPA* that provided for full disclosure to special advocates. With these changes, special advocates are prevented from serving their constitutionally required roles in accordance with the Supreme Court of Canada's holdings in *Charkaoui* and *Harkat*.

---

[85] *Charter* Application, *supra* note 30.
[86] *Ibid*, at para. 18.
[87] *Ibid*, at para. 19.
[88] *Charkaoui*, *supra* note 79.
[89] *Harkat*, *supra* note 67.
[90] *Charkaoui*, *supra* note 79.

If a special advocate is denied access to certain information, it also interferes with the judge's gatekeeper function, outlined in *Harkat*,[91] by impeding their ability to ensure that the record supports non-disclosure of the information and that the process is fair.

In addition, the changes to the *IRPA* give the Minister virtually unfettered interim rights of appeal regarding orders made for disclosure of information. While the protection of information touching on national security is certainly a pressing and substantial goal, the delays in judicial determinations that will be occasioned by broad appeal rights on behalf of the Minister may be highly prejudicial to named individuals. The appeal rights are also asymmetrical, putting the named person at a further disadvantage in cases where orders for disclosure have been refused.

The *IRPA* amendments call into question the constitutional validity of the security certificate regime, which has already been the subject of significant litigation. Not only are these changes incapable of being appropriately balanced by safeguards, they also backpedal on and interfere with the efficacy of those safeguards, like the special advocate program, which were implemented to protect fundamental freedoms.

[91] *Harkat*, *supra* note 67, at para. 46.