National Security Online Consultation
ICLMG's answers

Acronyms & Glossary

CSIS: Canadian Security Intelligence Services - human intelligence agency

SIRC: Security Intelligence Review Committee - review body for CSIS

CSEC: Communications Security Establishment Canada - electronic intelligence agency

OCSEC: Office of the CSE Commissioner - review body for CSEC

RCMP: Royal Canadian Mounted Police - national police

CRCC: Civilian Review Complaints Commission - review body for the RCMP

CBSA: Canadian Border Services Agency - has no oversight or review body

ATA, 2015: *Anti-terrorist Act, 2015* (formerly Bill C-51)

Charter: Canadian Charter of Rights and Freedoms

SCISA: *Security of Canada Information Sharing Act* (was enacted with the adoption of C-51)

SATA: *Secure Air Travel Act*

IRPA: *Immigration and Refugee Protection Act*

PPP: Passenger Protect Program

NSA: National Security Agency (American counterpart to CSEC)

IP address: Internet Protocol address - a unique computer identifier

IMSI: International Mobile Subscriber Identity - a unique cellphone identifier

SECTION 1: ACCOUNTABILITY

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

The existing review and complaint regime is inadequate and obsolete. Only certain agencies have a review body. CBSA, for instance, has no watchdog body; other agencies, such as CSEC, have very limited, weak and inadequate oversight. It is time to completely reform and renovate Canada's oversight and accountability regime.

Existing national security review bodies should be replaced by a single integrated and independent review and complaint mechanism with full authority, powers and resources to conduct detailed reviews and investigate complaints over all law enforcement and intelligence agencies and government departments involved in national security operations. Canada's 'whole-of-government' approach to national security must be matched by a 'whole-of-government' approach to review and accountability. However, this should not be to the exclusion of creating oversight bodies for non-national security related issues. For example, immigration experts have long called for an oversight and review body for CBSA in the entirety of their activities. We would argue, therefore, for the creation of both a single, integrated national security review body, as well as for a separate review body for CBSA-specific complaints and concerns.

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

A single integrated independent review and complaint body on national security would address this issue.

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

A new integrated independent review mechanism would have jurisdiction over all agencies (including CBSA) and government departments that have national security responsibilities.

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

While the creation of a Committee of Parliamentarians on National Security to ensure the democratic oversight of national security agencies and operations is welcomed, it must be seen as a complimentary mechanism, not a substitute for an independent expert review and complaint body. A committee of parliamentarians will focus on broad

oversight of the national security regime and operations, and related policy matters. It will not have the resources or capacity to carry out after-the-fact thorough reviews or investigate complaints. Parliamentarians are busy with their parliamentary obligations and cannot develop the expertise, nor allocate the time and energy, to carry out detailed in-depth reviews and investigations that only an independent and well-resourced expert body can carry out.

- **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?**

The creation of a Committee of Parliamentarians responsible for political oversight and of an integrated independent review and complaint body should be complemented by the appointment of an independent National Security Legislation Monitor, like in the UK and Australia. The mandate of this third expert mechanism would be to issue reports on government performance under anti-terror law and to examine the necessity and usefulness of existing laws and the need for law reform.

SECTION 2: PREVENTION

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

The mandate should be the prevention of violence, period. The government's focus on "radicalization to violence" rather than violence itself is counter-productive, stigmatizing for the populations targeted and a slippery slope. The United Kingdom government has already gone that way, moving from their already very controversial de-radicalization programs, *Prevent* and *Channel*, to a recent emphasis on combating "non-violent extremism." The government defines this as "opposition to fundamental British values." "British values" (just like "Canadian values") have never been properly defined, and by branding all opposition to them as extremist, the government is effectively outlawing dissent.

We have seen an alarming trend in governments' discourses - including our own – toward marginalizing protesters and activists (especially students, Native peoples and environmentalists), as well as rising islamophobia in Canada. In this context, we must stay away from any language or methodology that conflates particular ideas, political leanings or religious beliefs with radicalism and a propensity for violence.

Finally, more and more studies have shown that there are no accurate profiles for terrorists and no definite indicators for "radicalization." Studies have also disproved the links between religious beliefs and terrorism. Moreover, a recent FBI study into what motivates terrorist actions has found that the largest factor (although it was only in 18% of cases) is oppressive and structurally violent domestic and foreign policies put forward by governments, and the violent quashing of dissent against those same policies. The government of Canada must therefore make it a priority to ensure all policies are not only respectful of human rights, but also contribute to promote and further them.

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

The Government should take a leading role in challenging the fear-mongering which leads to suspicion of other cultures or religions, profiling of communities, and hate speech/hate crimes. Terrorist violence and individuals allegedly traveling to join terrorist groups abroad are much rarer occurrences than racist or sexist violence. An office that focuses almost solely on radicalization to violence linked to "Islamist" terrorism would simply contribute to solidifying the fear of terrorism, and stigmatize Muslim communities. The Government should instead create a national plan for the prevention of all forms of violence, focusing on both speech that calls for or promotes violent acts as well as, of course, acts of violence themselves – including police brutality and violence against women, specifically violence against Indigenous women. Such a body should also have

an anti-oppressive framework in general and take a clear position against sexist, racist, homophobic, transphobic and islamophobic speech. The government and its institutions should also lead by example and be respectful of human rights and repair the damage and abuse that's been done in the past, especially regarding the abuses committed in the name of national security as well as the treatment of Canada's Indigenous communities.

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

Prevention of violence is a social issue, different from policing. Police should be involved only if there is a real risk of violent actions. Otherwise, the involvement of police can be counter-productive, as we have seen in several US Countering Violent Extremism (CVE) programs, where individuals do not want to discuss their views due to fears of surveillance or prosecution; for many legitimate reasons, they do not trust the police. We've also learned recently that former employees of the Centre de prévention de la radicalisation menant à la violence (CPRMV) in Montreal were pressured by the director of the centre to violate their code of ethics by sharing all confidential information obtained from allegedly radicalized individuals in a centralized file the director had access to, and refused to say how that file could or would be used.

The Government can instead help by adopting anti-oppressive and inclusive policies; increasing funding to social services, education, healthcare, housing; and by generally improving infrastructure, employment opportunities and living conditions for all.

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

Assessing the particular needs of communities touched by violence is important. Consultations and studies are essential; it is important to note that many have already been carried out in the past by other organizations. However, moving forward, it is important that this work is not focused simply on radicalization to violence, but on the general needs of communities that will allow people to live better and healthier lives.

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

Studies have already shown there are no precise or full-proof indicators of radicalization. Any attempts to profile people for propensity to radicalization therefore becomes too broad and ends up targeting dissent. Providing funds for research into how to effectively counter hateful and violent narratives on the internet could be useful,

but the main focus should be on how to effectively eliminate poverty, inequalities, illness, and oppressions in general.

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

For the most part, this question is for individuals to answer according to the needs of their own communities.

However, there are some over-arching concerns we'd like to highlight. At the forefront is how the language and definitions used by government and media, among others, can lead to the stigmatization of communities – and absolving others.

First, we support the National Council of Canadian Muslims in its call for media and government to use "Daesh," rather than "Islamic State," when describing the terrorist group. Doing so removes any legitimacy or credibility it received by referencing either Islam or being a state. It also makes clear that they are not representative of Islam or the Islamic community, in Canada or internationally.

Second, a reflection on the definition and application of the word "terrorism" is necessary. Government officials, politicians and the media described the violent acts perpetrated on Parliament Hill and in St-Jean sur le Richelieu in 2014 as "terrorist" acts. These incidents were carried out by two recently converted Muslim men who watched Daesh propaganda videos but had no links to the group, acted alone and possibly dealt with mental health concerns. But the term terrorism was not used in describing the actions of a Christian man who killed three RCMP officers in Moncton in 2014, despite his espousing plans to overthrow the government, nor in regards to two white supremacists who, in 2015, planned to open fire on people in a Halifax mall. In the latter case, then-Justice Minister Peter Mackay said that "terrorism" did not apply because there was no "cultural" element to their plan (ignoring the fact that "culture" is not included in the criteria for a terrorist act).
There exist many violent actions that cause fear and terror in our communities which would not legally qualify as "terrorism", only furthering confusion and also division regarding what should be made a societal and governmental priority. For example, violence against women is widespread and must be addressed. And although eighty percent of these violent incidents occur in private residences, during the day, at the hands of men these women know, we collectively tell women that they must be afraid of strange men or to not go out alone at night. The actual violence and the overblown perception of the risk of violence put many women in a state of fear while out at night or in their general interactions with men. We would be much better served in addressing the root causes and de-mystifying violence that affects large parts of our society, rather than focusing on applying new, subjective labels.

SECTION 3: THREAT REDUCTION

- **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 those threats?**

We would first ask that the government define and quantify the threats referred to. In order to justify changes in CSIS' mandate and activities, we must first understand whether they are proportional to the threat to be addressed. To date, neither the government nor CSIS have presented compelling evidence in this regard. On the other hand, statistics continue to show that violent crime in Canada (in general) is decreasing. There have been two attacks classified as terrorism on our soil, and reports of approximately 160 people traveling to allegedly fight along-side Daesh. If this is the extent of the threat, we do not see the proportionality in granting new powers. Violence against women, again, is a much more prevalent threat and we see little action to substantially address this issue. We believe we need more justice, not more police powers.

Furthermore, giving CSIS threat reduction powers brings us back 40 years when the RCMP broke into and entered Parti Québécois (PQ) offices to steal members list, burned a barn, and put out counterfeit Front de Libération du Québec (FLQ) press releases in order to counter the separatist threat. One of the objectives in creating CSIS was precisely to put an end to such inacceptable acts in a democratic society. The role of CSIS must be limited to intelligence. The security of Canadians rests on the enforcement of the Criminal Code by the police.

- **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?**

Documents made public in 2014 (*Toronto Star*, 2014/09/18) revealed that since 2006, 800 demonstrations and events had been subjected to the scrutiny of government agencies and departments. The range of events that were targeted was very broad and were typical of a vibrant democratic society. They included a union demonstration, a public forum on the tar sands, a workshop on civil disobedience, a vigil on disappeared and murdered Indigenous women, and a fishermen's demonstration in the Maritimes. The threat reduction powers given to CSIS by ATA 2015 are a threat to the rights and freedoms of Canadians and must be revoked. Furthermore CSIS intelligence gathering must not target Charter protected activities such as the ones mentioned above. Sections 12.1 and 12.2 of the CSIS Act should be revoked.

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

A recent Federal Court decision concluded that CSIS had engaged in illegal bulk collection and retention of data on Canadians. The Court also concluded that CSIS had not shown candor in carrying out its mandate. The real priority is ensuring that CSIS respects Canadians' protected rights while fulfilling its mandate. Clearly, existing mechanisms are inadequate to insure CSIS compliance with the Charter and an independent review body capable of examining all the government agencies involved in national security is absolutely necessary.

SECTION 4: DOMESTIC NATIONAL SECURITY INFO SHARING

- **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?**

While the Government has expressed its commitment to ensure Canadians are not limited from lawful protest and advocacy, we have yet to see concrete actions that go in this direction. For example, while the government has put an end to new audits of charities, it has allowed outstanding audits to continue – a contradiction made to statements when in opposition. Legal measures continue to be used to silence dissent of First Nations towards projects like the Site C dam. And the government supported a motion condemning the legal right of Canadians to use boycotting as a way to display their opposition to a country's violation of human rights. None of these go in the direction of ensuring our rights to protest and advocacy are protected.

Regarding SCISA specifically, it should be repealed. The act facilitates the sharing of information on all Canadians amongst up to 17 government agencies for "activities that undermine the security of Canada and other countries." These activities, according to the definition in the Act, include a wide range of acts that are not remotely related to terrorism, such as activities that "threaten the country's economic interests and financial stability." Even if there is an exception for legitimate protest and dissent, the above definition of "threat" could include illegal labour strikes, civil disobedience protests (such as roadblocks to a pipeline project) and even economic boycott initiatives. This last example is particularly important in light of the recent motion condemning the Boycott, Divestment and Sanction (BDS) movement. It also allows information sharing with foreign governments without meaningful safeguards on the use of information, or any oversight, review or accountability for mistakes, potentially leading to serious human rights abuses such as in the cases of Maher Arar, Ahmad El Maati, Abdullah Almalki, Muayyed Nureddin, and Benamar Benatta. This means that all Canadians – including those engaged in legitimate political activity – are placed in danger. The only solution is repeal.

- **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?**

This wouldn't change the risks mentioned above. Repeal is the only solution.

- **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?**

The review mechanisms in Canada are not sufficient; they were not before information could be shared between 17 departments, and they are even less so now. Further Bill C-22, establishing a Committee of Parliamentarians, will not fix this either. The Office of the Privacy Commissioner (OPC) is just one level of accountability; in order to provide sufficient accountability, an overarching review mechanism must be established (see our response on accountability for more details).

Regarding the OPC, the office should be allowed to conduct a privacy assessment of legislation before it is tabled. Information sharing between government departments should be the subject of a prior assessment on the part of the OPC, and the office's recommendations should be binding. The resources of the OPC should also be augmented to meet the increased challenges to privacy.

- **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?**

That this was not already included in the legislation, or required before, is highly problematic. However, as we have seen regarding the record keeping habits of CSIS and CSEC, such a regulation would not be sufficient to 1) ensure that record keeping happens and 2) make SCISA less risky or more accountable. The Act should be repealed.

- **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?**

It is obvious that sharing information between so many entities will lead to abuse, especially since it is based on mere suspicion of activities, and predicated on a new, enlarged definition of "threat to national security." Moreover, even before the adoption of Bill C-51, the sharing of information lead to abuse. Better safeguards must be in place, and SCISA should be repealed.

Besides the troublesome domestic information-sharing allowed by C-51, the lack of debate and regulation around information-sharing in the context of the North American Security perimeter and Canada-US border agreements is unacceptable. A huge amount of Canadians' private information, including airline passengers' information on most domestic flights, is now shared with US Homeland Security. Once in the hands of US authorities, this information can be shared among 17 US agencies and is not protected by Canadian privacy laws.

SECTION 5: PASSENGER PROTECT PROGRAM

- **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 subsequently be removed from the List?**

The necessity, usefulness and efficacy of Canada's No-Fly List regime has not been demonstrated and the program should be abolished. Furthermore the listing process appears to violate the Canadian Charter of Rights and is characterized by many flaws with regards to due process and the principles of fundamental justice. We are concerned by the fact that the people putting names on the list are also the people tasked with reviewing that decision; that people are only notified that they are on the list if they try boarding a plane and are stopped; that the regime does not define a clear and efficient way of recourse for individuals on the list; and that many if not most Canadian airline companies also use the American no fly list, for which recourse seems even less clear and efficient (and, moreover, raises questions regarding the principle of sovereignty).

The process of application for removal is also plagued with a lack of procedural fairness. Even the proposed appeal to the Federal Court, modeled after IRPA's security certificate regime, would not meet the requirements of the Supreme Court ruling in Charkaoui. However, until PPP is abolished, individuals seeking removal should be removed from the list automatically if the Minister does not decide within the 90 days after an application is filed. Canada should repeal the *Secure Air Travel Act* and keep suspected terrorists away from airplanes using the existing tools under criminal law.

- **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?**

While news reports recently suggested that the government is moving in this direction, we remain concerned that it will take up to 18 months for such a system to be in place. There will also remain the need to address the issue of Canadian airline companies using the US no-fly list, to ensure redress for Canadian travelers facing unwarranted restrictions from foreign governments, and to get rid of the no fly list regime altogether.

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

No procedural fairness in appeals is possible unless an individual is presented with all of the evidence, or intelligence, in order to meet the case. In fact, if PPP is not abolished, it should be amended to reflect the practice in other types of court restraining

orders. To list someone, the government should need to seek a court order from a judge at the time of the listing, and the individual presented with the opportunity to respond to the case at that time.

Further, action should be taken so that the US list does not apply in Canada, given that the US no-fly list regime is equally flawed. Until it is abolished, Canadians placed on the US no-fly list should receive proper recourse and help from the Canadian government to defend themselves.

SECTION 6: CRIMINAL CODE TERRORISM MEASURES

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

The ATA, 2015 lowers the existing thresholds for preventive arrest and peace bonds, lengthens the amount of time someone can be held (from 3 days to 7 days), and provides for the imposition of harsher conditions once released, all with no criminal charge. The peace officer will only have to believe that a terrorist activity “may” be carried out and to “suspect” that the detention is “likely” to prevent a terrorist activity. “May” could simply be speculation and “likely” a mere hypothesis.

There is also the problematic issue of investigative hearings under Section 83.28. This section allows a police officer to bring a person before a judge in order to compel him or her to answer questions raised by the police. This introduces inquisitorial judicial procedures in the Canadian justice system, a totally new paradigm concerning relations between the state, the police, the courts and the citizens. In Canadian Common law we have an adversarial system. Investigative hearings are a breach in the independence of the courts and the justice system. Under these procedures the judge becomes an instrument of the state. Such procedures are usually associated with totalitarian regimes. The persons targeted by these measures will be associated with terrorism in the mind of the public although they have not been convicted of anything. This is reminiscent of McCarthyism in the US.

Allowing individuals to be subjected to severe restrictions to their liberty without a criminal charge – much less a conviction – was already permitted under existing Criminal Code provisions before 2001.The measures introduced in ATA, 2001 and extended in ATA, 2015 should be repealed.

- **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?**

This crime of advocating and promoting is so vague that a person who discusses terrorism issues or repeats the words of a group on a terrorist list could be targeted, even though they don't support that group in any way. This will push individuals towards self-censorship and stifle public debate on issues of terrorism. In particular, academics and journalists could choose to address less controversial issues or be forced to reveal the identity of research subjects or sources who would otherwise have remained confidential.

The list of existing terrorism offences in the Criminal Code is already extensive and includes facilitating, participating, instructing, harbouring, financing and counselling. If the offence of counselling already exists, why modify a problematic promotion offence to make it more like counselling? This section must be repealed.

- **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?**

The ATA, 2015 provides for the seizure and destruction of terrorist propaganda defined in very broad and ambiguous terms. The primary impact of this new offence will be to chill legitimate speech and send suspicious online expression – which can provide valuable leads for intelligence agencies and law enforcement – underground. This measure is similar to the infamous Padlock law of Maurice Duplessis in Quebec. The whole section should be repealed.

- **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?**

Protections for witnesses were already adequate before the adoption of the ATA, 2015; the protection of witnesses should not counter the need to repeal C-51. However, if it is demonstrated that more protections are necessary, they should be introduced in a new bill, and properly debated.

There are also concerns regarding the use of witness protections to extend to sources of national security agencies. Specifically regarding the Protection of Canada from Terrorists Act, 2015 (previously Bill C-44): it requires that CSIS's human sources remain confidential, even to the judge, unless a court orders otherwise. This is despite a clear finding by the Supreme Court of Canada in *Harkat* that this protection was not necessary given the broad powers that prevent public disclosure of harmful information under the IRPA. Furthermore, it prevents defense lawyers from cross-examining sources, and prevents the accused from knowing the full case and evidence against him or her. Finally, C-44 created a blanket rule for all kinds of procedures, regardless of their nature, scope or source of information. As others, including the Canadian Bar Association, have argued, this kind of blanket regulation ignores the nuances in different types of proceedings, including criminal prosecution, immigration or security certificate proceedings. It makes no attempt to strike a balance between national security and civil liberties.

This section of C-44 should be repealed, along with C-51, and no further "protections" should be awarded to national security witnesses or sources unless proven necessary.

SECTION 7: PROCEDURES FOR LISTING TERRORIST ENTITIES

- **Does listing meet our domestic needs and international obligations?**

It is difficult to conceive how listing meets domestic needs, since for instance none of the listed entities pose a fundamental threat to Canada. Most listed entities are foreign groups involved in national or regional conflicts who would never direct their activities against Canada if we did not intervene in those conflicts (fuelling possible retaliation). Also, because the listing process rests on a sweeping definition of "terrorism," it fails to distinguish between criminal terrorist entities and freedom fighters or liberation movements, whose legitimacy can shift depending on the time period and the dominant political interests concerned. Under the current definition, Nobel Peace prize recipients Nelson Mandela and Rigoberta Menchu would be considered terrorists. Members of the French resistance fighting against the Nazi occupation would have fallen into the same category. Inversely, the definition fails to address the issue of state terrorism that, in fact, is carried out against their own people by some of the very countries that have joined the U.S.-led campaign against terrorism.

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

Because listing is fraught with problems related to the definition of terrorism and the subjectivity of political interests at any given point in time, it should be abandoned in favour of prosecution for concrete criminal acts, including conspiracy, which were already covered under Canada's criminal code prior to the tragic events of September 2001 in the US. Furthermore, no listing regime can protect Canada from the threat of criminals seemingly suffering from mental health issues and acting alone, which is what we have faced so far in Canada.

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

It is difficult to conceive how listing contributes to reducing criminal acts labelled as "terrorism". Listing cannot replace good intelligence and police work.

While we would argue for the abolishment of the listing process, we would also guard against moving towards the system currently used by Citizenship and Immigration Canada (CIC). While the CIC does not have a formal "terrorist entity" list, it does allow individual functionaries to evaluate and decide whether an individual's political affiliations disqualify them from immigrating to Canada. Such an arbitrary procedure is even worse than listing, in that in this case there is no benefit of knowing which organizations are or are not listed.

We would argue, then, that the concept and definition of groups as terrorist entities be completely abolished, whether in the Criminal Code or in IRPA, in favour of evaluation based on concrete, clear criminal acts.

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

The present listing process under the ATA, 2001 appears to violate the principle of procedural fairness guaranteed by the Charter of Rights and Freedoms. The process makes it impossible for an individual or an organization to challenge the listing since all their assets are seized and cannot even be used by the listed entity to retain legal counsel. Furthermore, the listing is often based on intelligence sources or information from other countries (rather than evidence) that cannot be cross-examined in court, especially in the context of secret hearings based on IRPA's certificate regime. Listed entities should know the full case against them in order to be able to meet the case.

SECTION 8: TERRORIST FINANCING

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

In its 2009 and 2013 review of the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Office of the Privacy Commissioner found several unsatisfactory aspects in the Centre's data collection and retention policies, putting at risk the privacy rights of Canadian citizens, permanent residents and foreign nationals. This included weaknesses in FINTRAC's guidelines and procedures in working with private sector partners.

In particular, the OPC found that in at least one instance, FINTRAC's guidance to private sector partners on the implementation of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) could be interpreted as encouraging the reporting of information that is not required by the Act. Further, it found that FINTRAC, which holds responsibility for the implementation of the Act's requirements among its regulatory partners, has failed to review the guidelines issued by these partners, meaning that there is no way to ensure that the guidelines are compliant with the Act.

Faulty guidelines and lack of oversight put both the private sector at risk of fines for non-compliance and threatens the privacy rights of Canadians by collecting and retaining private information that is outside the scope of the FINTRAC's mandate.

These issues were first identified by the OPC in its 2009 report and have yet to be adequately addressed by FINTRAC. A review of FINTRAC's 2014 and 2015 annual reports shows no update on, or even recognition, of these issues.

We would recommend that FINTRAC act quickly to address the concerns as reported by the OPC in their report, *Financial Transactions and Reports Analysis Centre of Canada, Section 37 of the Privacy Act, Section 72(2) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act, Final Report 2013.*

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

Once again, we would point to the OPC's 2009 and 2013 reports on FINTRAC. By issuing clear and complete guidelines, and reviewing the guidelines issued by reporting organizations to their staff, FINTRAC would significantly strengthen its relationship with the private sector.

Further, the OPC's reports also raises questions about front-end screening of data that is transmitted to FINTRAC. Currently, while the forms to be filled out have requirements for necessary information, there is no review for over-reporting of information. As the OPC suggests, having front-end screening would clarify what information is relevant for

collection and retention purposes, clarify what is required of private sector and regulatory partners, and ensure that the privacy rights of Canadians are protected.

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

We would argue that in the case of FINTRAC that no, the safeguards are not sufficient in protecting individual rights or the interests of Canadian businesses. Again, a lack of clear guidelines puts Canadian businesses at risk of over-collecting and over-reporting information. In an instance where this would breach the PCMLTFA, it would put the business at risk of substantial fines. Even more worrisome is the lack of clear guidelines and of front-end screening, as mentioned earlier, which means that the private information of Canadians is being collected and stored by FINTRAC without adequate oversight that this information is within their scope. The OPC found that extraneous information, such as Social Insurance Numbers were collected although FINTRAC is not supposed to, as well as reports that did not fit the reporting criteria. This included instances where reports of cash transaction, electronic funds transfers and CBSA reports did not meet the $10,000 reporting threshold and therefore should not have been reported, and reports that did not include the entity's reason for suspected money laundering or terrorist financing activities, making it difficult to assess whether the "reasonable grounds" threshold had been met.

As of 2013, FINTRAC held some 165 million records. Because there is no electronic screening method for these records, it is impossible to know how many of these records are compliant or how any are extraneous and should be destroyed. As the OPC reports, FINTRAC informed it that only those records that are selected for further analysis are ever reviewed. Once they are reviewed, if the information is not relevant it is still stored for the mandatory 10 years as laid out in the PCMLTFA – meaning that even non-relevant information is still not destroyed; indeed, FINTRAC is currently working on a system that would simply segregate this information from the main database so it cannot be accessed by analysts. FINTRAC advised the OPC that they will be implementing a process to automate the identifying and disposing of these types of reports. We urge them to do so as soon as possible.

The sole heartening information is that the OPC recognizes that FINTRAC is correctly following guidelines governing the release of information to security agencies. Therefore, non-compliant information remains securely stored at FINTRAC and is not unnecessarily shared with security agencies. At the same time, two concerns remain: First, whether SCISA has made it easier for other security agencies to request the disclosure of information, or lowered the threshold for what FINTRAC can voluntarily disclose – this should be clarified as soon as possible. Second, the large-scale accumulation of private information remains a grave risk for the privacy rights of Canadians: future incidents could make this information available to either security agencies or to malicious parties. Extraneous information should not be collected in the first place, but, if it is collected, it should be identified and disposed of as quickly as possible.

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

We would urge FINTRAC to adopt the recommendations of the OPC as soon as possible in order to ensure:

- Reports from reporting organizations are as compliant as possible, contain only relevant information, and explain the reasons for reporting. This would include improving guidelines issued by both FINTRAC and reporting agencies
- That all non-compliant records are identified and disposed of as soon as possible
- That all records that are not part of disclosures are adequately disposed of after the 10 year retention period

We would also urge FINTRAC to report openly on these issues in their own annual reports, rather than simply responding to the OPC in their two-year reviews. Ensuring that only relevant information is collected and stored will help in upholding privacy rights, limit any potential future breaches, and also increase the efficiency of FINTRAC's monitoring work.

We would also like to note that an increased focus on money laundering as well as tax havens would most likely serve the purpose of reducing funds for crimes, as well as increase the Canadian tax-base. A reinvestment of this new source of taxes into social services could help reduce the social inequalities that often lie at the root of what are seen as terrorist acts, and therefore serve as a just as – if not more – effective method of increasing the security of all Canadians.

Finally, we would urge the government to create an oversight and review body for FINTRAC to ensure it is compliant and that could receive complaints. In regards to their national security-related work, we would argue that this fall under an eventual integrated, independent review and complaint body for all national security agencies, as proposed in Section 1: Accountability.

SECTION 9: INVESTIGATIVE CAPABILITIES OF THE DIGITAL WORLD

- **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?**

The Government should adhere to decisions of the Supreme Court and the findings of the Office of Privacy Commissioner, and engage on a sustained basis with legal experts and human right and civil liberties organisations for guidance into addressing challenges while respecting the Charter and international human rights obligations.

- 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. Should investigative agencies operate any differently in the digital world?

The digital world and the physical world are very different: the former is infinite and the latter is very narrow. As such, a warrant allowing search and seizure in a home will not necessarily be able to give access to private information such as bank or medical records that a warrant for a digital device would. If digital access is needed for an investigation, it should be limited to what security agents are looking for in order to directly prevent or prove a specific crime. It should not apply to a device in its entirety, which could lead to important privacy violations.

- **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?**

The Snowden revelations and the work of several journalists and newspapers have revealed that investigative agencies already possess and use too many intrusive technology and tools to access information in the digital world. Canada's national security agencies' capability to conduct mass surveillance, legally or illegally, has highly contributed to the ongoing erosion of privacy and Canadians' Charter rights. These tools should actually be scaled back.

For example, CSEC helped the NSA to create a "back door" in an encryption key used worldwide, has spied on Canadians using public WiFi networks, has captured millions of downloads daily, has engaged in mass Internet surveillance of file-sharing sites, has developed cyber-warfare tools to hack into computers and phones all over the world, and has shared information on Canadians with its foreign partners without proper measures to protect privacy.

More recently, a SIRC report analyzed a little-known program of bulk data collection operated by CSIS since 2006. Two troubling points were revealed: First, SIRC

disagreed with CSIS over the agency's classification of some of its bulk data collection of private information as "publicly available" and "openly sourced," for which CSIC claim they do not need to meet the "strict necessity" requirement for data collection. Second, and even more troubling, was SIRC's finding regarding the datasets that CSIC classified as meeting the requirement of "strict necessity": "SIRC found no evidence to indicate that CSIS had appropriately considered the threshold as required in the *CSIS Act*." It is impossible to read this as indicating anything other than contempt for the law. This is so serious a matter that SIRC called for the immediate halt to the acquisition of bulk data sets until there is a system in place to confirm compliance with the law. A Federal Court recently ruled that this bulk data collection is illegal. Media have reported that Minister Goodale is contemplating changing the law so that CSIS can use this data. Laws should not be modified to legalize a problematic practice and allow more invasion of privacy. The collection should stop at once and CSIS should respect the law.

Finally, we are also concerned by law enforcement agencies, including the RCMP, using IMSI catchers - or stingrays - which are devices that can identify any cellphone in their vicinity. Despite being in use since at least 2005, and despite the fact that they can disrupt calls – including causing 50% of 911 calls to be dropped – the Canadian Radio-television and Telecommunications Commission (CRTC) was not aware of their use by law enforcement. There must be more transparency and regulations around the use of IMSI catchers and other new surveillance technology.

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

Absolutely. It is higher for the digital world, for the reasons specified above.

<u>Basic Subscriber Information (BSI)</u>

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

There is a reason the Spencer decision limited access to BSI: to protect Canadians' privacy rights. That ruling must be respected and police and national security agencies should obtain a warrant at all times when they want BSI, even when the telecommunications companies would otherwise give it voluntarily. In some true emergency situations (i.e. if a life is in danger or a crime is about to be committed), the criminal code already allows police to access BSI without a warrant.

According to digital privacy experts Tamir Israel and Christopher Parsons, in keeping with past attempts to introduce an unfettered digital identification power, the consultation documents have failed to make the case that such indiscriminate powers are needed. The documents repeat long enduring claims that current access mechanisms are 'inconsistent and slow', but fail to acknowledge the fact that such claims have been repeatedly discredited in the past.

Finally, in the context of this national security consultation, unfettered access to digital identifiers is presented as a national security measure intended to address critical counter-terrorism matters that are currently at the forefront of national attention and concern. However, as in past attempts to introduce this legislation, the power proposed is one of general application, meaning it will be used predominantly in other investigative contexts. Further, no specific explanation is provided for why this exceptional power is necessary even in the national security context. Indeed, upon the 2013 defeat of this proposal as embodied in Bill C-30, then Director of CSIS indicated that unfettered access to subscriber identification information is "not absolutely critical for us to do our work." While on the one hand these identification powers may not be 'absolutely critical' to national security, their indiscriminate availability to agencies such as CSIS and CSE can have even more serious and far-reaching privacy implications.

- **Do you consider your basic identifying information identified through BSI (such as name, home address, phone number and email address) to be as private as the contents of your emails? your personal diary? your financial records? your medical records? Why or why not?**

Yes, absolutely. BSI also includes IP addresses and mobile devices' IMSI number, and can reveal intimate details of a person's contacts, networks, activities, lifestyle preferences, whereabouts, etc., when linked to other information. This is the opinion of the Supreme Court of Canada, and multiple evidence-based research reports have demonstrated its far-reaching capacity to invade. Replicating a trend that is regrettably evident throughout the consultation documents, the documents treat privacy in subscriber information as, at best, an afterthought. By ignoring the rich and detailed historical debate that has occurred in Canada on this matter the government has failed to acknowledge the privacy issues associated with indiscriminate access to digital identification.

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

Yes there is a difference. In the digital world an IP or e-mail address, when linked to other information, can reveal an infinite amount of intrusive intimate personal information.

<u>Interception Capability</u>

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

According to digital privacy expert Christopher Parsons, the police have their own equipment that is capable of integrating with telecommunications carriers' equipment, and they have the competence to install it when a carrier does not possess the surveillance capacities desired. That federal authorities have to expend their own funds to initiate such surveillance is not inherently bad, since it forces authorities to engage in a careful evaluation of where best to expend limited public funds: this means that authorities will, presumably, prioritize high-risk cases as opposed to initiating a broad surveillance infrastructure. Such economic rationales are one of the ways that society ensures police are circumspect in how broadly they engage in surveillance. With that knowledge, the concerns related to privacy intrusions and the unnecessary burdens on the communications industry (and the consumers) seem justified.

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

With a warrant, this should be allowed. However, apart from what was said in the previous response, many Canadians have also lost confidence in our national security agencies, and question their respect for our right to privacy. Recently, the public was also informed of problems of diligence among justices of the peace when issuing warrants to spy on journalists (who are not suspected of any crimes). Therefore, interception powers should be severely limited to the communications between people suspected of planning or having committed a crime; not all the communications of those people with others. Just like it's not acceptable to open and read all letters received by an individual, it should not be acceptable to open and read all the emails of an individual. If there are communications intercepted by mistake that are not related to the crime, they should not be kept or used.

<u>Encryption</u>

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

Compelling decryption could necessitate a key that will unlock the data or communications of all a company's users. This creates a huge risk of privacy violations,

and is a dangerous slippery slope towards government access to private information in general.

This proposal also rests on a violation of one of our most fundamental rights: our right against self-incrimination. It is very difficult to imagine how a law that would compel a password could be constitutional. No proposal should even be explored until we have court decisions on compelled passwords in the context of inspections by the Canadian Border Services Agency. These are cases that are already in play and will provide important guidance. If compelling a password isn't constitutional in the context of border security, it will not be constitutional in the setting of ordinary criminal law. Finally, it has also not been demonstrated that this is necessary to conduct effective investigative work.

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

That appears to be impossible. Encryption needs to work all the time, otherwise it's not really encryption. It is now commonplace to hear law enforcement state that encryption is a barrier to their investigations. However, our entire digitally-mediated world requires strong security, so that criminals and foreign governments and rival businesses are less able to conduct surveillance on Canadian citizens: encryption keeps us all safer. We have too great a need for cyber-security to undermine it in this way.

Furthermore, recent suggestions in the media that encryption has prevented investigations from going forward, or that decrypting certain data would have been useful, are problematic. In fact, several of those investigations did not stop after facing the barrier of encryption. Also, without knowing *what* was encrypted, there is no evidence that encryption was a significant problem, only that there was some information that could not be readily accessed.

<u>Data Retention</u>

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

The police already have the power to obtain a Preservation Order, which a judge can grant based on a low threshold, and allows the police to require preservation of information in particular cases. For example, cases in which it will take time to get a search warrant and the information is in danger of being destroyed. What the Green Paper asks is whether telecommunications companies should just be required to retain data for long periods of time, just in case the police need it**.** Rather like a global preservation order.

The 2014 Court of Justice of the European Union struck down the EU “Data Retention Directive” because the blanket retention of innocent persons’ data violates the EU Charter of Fundamental Rights. It is at least possible that it would violate our Charter as well. So evidence must be produced to show that current powers are insufficient before any consideration is given to a policy that has already been rejected in Europe as a violation of fundamental rights.

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

The Governement of Canada should not enact a general data retention requirement.

SECTION 10: INTELLIGENCE AND EVIDENCE

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

Section 38 procedures are complex and inaccessible. The current system, using national security and international relations as reason to keep information, intelligence and evidence secret and unavailable to defendants, is rooted in the concept of "state secrets" which is prejudicial against defendants in several ways. It can be used in civil suits when brought against the government: during the Arar Inquiry, state secrets were used to block investigations into government agents. It could easily be used in other cases of seeking redress for torture.

In criminal cases, it is understood that any system that denies direct access to the evidence presented against a defendant is a violation of the right to a fair and equitable trial. Moreover, once state secrets are invoked under s. 38, the case automatically changes venues to Federal Court (even if it was in Superior Court); this, despite the fact that the judge in a criminal case is the best suited to judge the relevance of evidence to be used against the accused. Because of the regulations and the secrecy, judges can accept intelligence, hearsay and other information that is normally inadmissible without the defendant ever knowing. This goes so far as to include information obtained under torture. Further, the minister in question controls the evidence. They have no obligation to share all the evidence – including any exculpatory evidence. There is no obligation to disclose. For example, in the cases of Adil Charkaoui and Mohamed Harkat, we know that CSIS destroyed original evidence, and entered into evidence only summaries. This falls far short of full disclosure. This system is inherently unfair and must be reviewed.

- **Could improvements be made to the existing procedures?**

A defendant should at all times have access to the evidence used against them in order to mount an adequate defence and to ensure a fair and just trial.

- **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?**

A defendant's lawyer should have access to the evidence presented against their client, be able to fully review and challenge that evidence in court. However, we would still argue that any system that allows for secret trials that prevent defendants from fully accessing the evidence against them is an unjust and unacceptable system.

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

As stated above, the over-extended use of secret information in our judicial system is a concern. These practices must be reviewed and scaled down. It is therefore highly undesirable to add measures that have not been thoroughly debated in Parliament but that would further the use of secret national security information.

- **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?**

Again, apart from allowing defendants full access to the evidence against them in order to ensure fair trials, the entire system that developed and has increased the use of secret national security evidence and intelligence must be reviewed, revised and most likely scaled back to protect our Charter rights and 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?**

Division 9 of the IRPA, commonly known as the security certificate regime, is a highly problematic provision that should be repealed. The use of special advocates or the role of the judges cannot repair a system that completely goes against the principles of fundamental justice and the right to a fair and open trial.

There are several concerns regarding those detained under security certificates, includng that they are:

- Imprisoned indefinitely on secret evidence, though no charges have been laid against them;
- Tried in unfair judicial proceedings where information is not disclosed to the detainee or their lawyer;
- Denied the full right to appeal when the certificate is upheld in a process that uses the lowest standard of proof of any court in Canada;
- Under threat of deportation even when they face unfair imprisonment, torture or death.

Although the latest Supreme Court of Canada decision in the case of Mohamed Harkat has upheld the security certificate against him, the justices have stated their discomfort with such a regime as the evidence against the person subjected to a security certificate is kept secret from them and their lawyer, and thus they are unable to respond to it. Such a grave concern should have lead to a declaration of the regime as unconstitutional, and we would ask, again, that it simply be repealed.

GENERAL FEEDBACK

- **What steps should the Government take to strengthen the accountability of Canada's national security institutions?**

What is needed is a new, integrated and single body with the mandate, resources and expertise to conduct detailed reviews and to investigate complaints over all law enforcement bodies, intelligence agencies and government departments involved in national security. Granting the independent review body jurisdiction to examine all national security matters within the federal government would empower it to follow the trail of intelligence, information-sharing, and other national security activities throughout government. There would be no need for complicated choreography between existing bodies, for the creation of new bodies for each and every implicated agency (unless necessary, like for CBSA) or for the discretionary appointment of public inquiries like the Arar, Iacobucci and Air India inquiries which had a whole-of-government mandate. Legislative reform would be required to create this entity.

This body with whole-of-government review powers must meet a number of democratic values in order to achieve legitimacy in the public's eye:

- It must be clearly independent of government and the national security agencies over which it has authority.
- It must be an expert body that deals with national security issues on a daily basis. As well, the new body must be adequately resourced and staffed in order for it to meet the challenge of effectively reviewing our national security agencies.
- It must be accountable to the public through annual public reports assessing whether and how our agencies have lawfully responded to threats to the security of Canada.
- The new review body should compliment the new committee of parliamentarians by making recommendations to the committee with respect to policy changes that would make our national security agencies operate more effectively and our review system more robust in protecting national security and the civil liberties of all people in Canada.

The kind of "on the ground" experience gained by this review body will greatly assist the committee of parliamentarians in confronting the systemic issues it will face in fulfilling its important mandate.

A third component of a robust accountability model would include the important and complementary addition of an Independent National Security Legislation Monitor capable of supporting the work of the Parliament, the National Security and Intelligence Committee of Parliamentarians and the expert review body. Both the United Kingdom and Australia have bolstered national security accountability by appointing such independent monitors of national security law.

- **Preventing radicalization to violence helps keep our communities safe. Are there particular prevention efforts that the Government should pursue?**

As was said above, the focus should be on preventing violence in general, not on radicalization. A national plan against all forms of violence – from domestic to racist to police violence – is necessary.

- **In an era in which the terrorist threat is evolving, does the Government have what it needs to protect Canadians' safety while safeguarding rights and freedoms?**

The Government already had all the necessary powers to face criminal threats of a terrorist nature in the Criminal Code before the adoption of the ATA, 2001. New “anti-terrorism” laws adopted since that time have been shown to violate human rights and civil liberties in one way or another. They have not proven to be either necessary or effective.

- **Do you have additional ideas or comments on the topics raised in this Green Paper and in the background document?**

The Green Paper, both in tone and content, appears biased in favour of the challenges faced by law enforcement and national security agencies, rather than reflecting a profound concern for democratic rights and freedoms. The document can be read as justifying existing measures in the *Anti-Terrorism Act, 2015*; this includes defending those items the government dubbed the "most problematic elements" and has promised to repeal. The Green Paper also makes several claims that the current tools at the disposal of law enforcement to access subscribers’ information are “inconsistent and slow,” where, in fact, such claims have been repeatedly discredited in the past.

Furthermore, there are several elements that shine by their absence: There is no mention in the Green Paper of CSEC and/or mass surveillance operations carried out with its Five Eyes partners, and this in spite of the Snowden revelations. There is also no indication that the government intends to implement the O’Connor Inquiry recommendation to create a robust and independent “review and complaint” mechanism for national security operations (as opposed to a Parliamentary oversight body). If it was needed 10 years ago, it is even more urgently needed today.

The Government should:

- Repeal C-51
- Make major amendments to Bill C-22 to empower a future committee of parliamentarians to carry out its oversight functions without ministerial veto and make it democratically accountable to Parliament
- Repeal the no-fly list
- Re-instate the principles of fundamental justice and due process in criminal trials and administrative tribunals
- Settle the lawsuit launched by torture survivors Almalki, El-Maati and Nureddin
- Implement an appropriate redress system for future victims of human right violations

- Repair the access to information system and be more transparent
- Put a stop to the creation and use of secret, internal interpretation of laws that regulate the activities of its national security agencies
- Create a Commission of Inquiry into Canada's policies and practices relating to the transfer of detainees to Afghan authorities
- Ensure that entrapment is not used by our law enforcement agencies
- Remove the torture memos.

Issues of privacy are also essential to this consultation. The Government should therefore also:

- Act on the concerns raised by the Office of the Privacy Commissioner of Canada with regards to potential new legislation that would facilitate surveillance in the digital world.
- Increase privacy protections so the government cannot simply pass laws each time it wants to retroactively legalize actions that have been found to violate privacy obligations (such as the recent revelation of CSIS bulk data collection).
- Stop using the right to privacy as an excuse to withhold information into the cases of Canadians detained abroad.
- Ensure better privacy protections for online communications between Canadians that have to pass through the United States of America because of the digital infrastructure.

We welcome the Government conducting consultations, and we hope that the results will truly inform future policies. However, we must express our concern that such consultations must be conducted in an efficient, timely manner. There is always the risk that consultations become drawn out and, by the time they are completed, the issues they were meant to be addressed become seen as entrenched and beyond the reach of repeal or even change. Furthermore, the consultations - including online discussions, MP town halls and audiences by the SECU Committee - are somewhat inaccessible, due to their length, language, lack of publicity, and the incredibly last minute announcements of their dates and locations. This should be remedied.

Finally, the Government should be transparent when it comes to the analysis of the data collected through this public consultation on national security by releasing all submissions and transcripts for public consultation and evaluation.