BC FREEDOM OF INFORMATION AND PRIVACY ASSOCIATION

National Security Online Consultation
Responses of the BC Freedom of Information and Privacy Association

SECTION 1: ACCOUNTABILITY

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

The current review bodies are restricted in jurisdiction to a reviewing a single agency. This is inadequate to the task and must be reformed. Most of the agencies or departments deemed important enough to national security that they are included in the *Security of Canada Information Sharing Act* are not covered by any review bodies whatsoever, and the ones that do exist have serious shortcomings.

Given the increasing propensity for the security agencies to work collaboratively, it is essential that a single body be empowered to review and investigate complaints against the ever-growing security apparatus as a whole.

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

See above re single integrated independent review and complaint body.

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

Again, the single integrated review body should have jurisdiction over all agencies and departments, including CBSA.

- **The proposed committee of parliamentarians will have a broad mandate to examine the national security and intelligence activities of all departments and agencies. In 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?**

The Committee of Parliamentarians is not an actual parliamentary committee, and it does not have any of the powers of a parliamentary committee. Please refer to the *Emergencies Act*, which provides for oversight and reporting by a joint Commons-Senate Committee during a war

emergency. If it is possible to have a real parliamentary Committee providing oversight and reporting to Canadians every 60 days during an actual war, it is unacceptable to have Canadians make do with this bastardization.

Even if there was to be a real parliamentary committee instead of what is being proposed in C-22, this body would not take the place of an independent expert review and complaint body.

What is needed in terms of accountability is a Parliamentary Committee, integrated expert review and an independent monitor (as in the UK and Australia).

- **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?**

As noted above, there should be an actual Parliamentary Committee, an independent review and complaint body able to look at issues and also an independent National Security Legislation Monitor, as has been established in the UK and Australia.

We also note the elimination of the CSIS Inspector General's office under the previous government has also reduced scrutiny over the activities of this part of the security apparatus. The claim was that this would save about $1 million, a pittance compared to the CSIS budget. This body acted as the Minister's eyes and ears in terms of what CSIS is up to, and its abolition means the Minister is even more dependent on the Agency to review itself.

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?**

What it should not be is a stealth program to ostracize and isolate people on the basis that they belong to a group government believes prone to violence. The emphasis should be on dealing with people who are violent or planning violent acts.

We do not want to see a Canadian version of the absurd UK program which resulted in school authorities turning in eight year old 'terror tots'.

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

The government should concentrate on protecting the population from violence, based on the criminal law which has served us well for centuries, including previous episodes of political violence.

The isolation of parts of our population on the basis of a 'propensity to violence' will only facilitate the task of those interested in creating followers, contrary to the government's stated objective.

Similarly, the identification of violent criminals as terrorists rather than murderers, extortionists etc. works to advance their narrative that they are not criminals but heroic freedom fighters.

- **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?**

See above. Do not set up a system that advances the narrative of violent criminals portraying themselves as heroes fighting a corrupt system.

Working with and listening to the communities, if genuine, could be a useful approach.

- **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?**

Perhaps you should try listening to the views of those communities as to what their needs are in terms of funding.

- **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?**

This should not become a cover for a 'Minority Report' style of identification of pre-criminals.

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

Not applicable.

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?**

The government has not set out a case for these broad additional powers beyond vague generalities, and has not shown how these powers and their clear infringement on civil liberties and *Charter* rights will actually reduce these threats.

There have been threats against the security of this country going back to the century before last, but the government and security apparatus claim the latest threats are somehow so different and extreme that it requires powers above and beyond any previously granted a government outside of wartime.

- **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?**

There have been repeated problems with CSIS obeying the law regarding its other activities (see decision of Justice Noel in Federal Court re lack of candour with the courts and the SIRC report on unlawful data collection and storage).

These additional powers need to be removed, that would be the most effectively safeguard.

- **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?**

CSIS was apparently unable or unwilling to abide but the standard of necessity set out in s.12 regarding bulk data collection. Apparently they preferred a standard of 'we might want to use this someday', despite the legal requirement that collection had to be necessary for its operations.

The concept of a Canadian judge signing a warrant pre-authorizing the violation of the *Charter* was abhorrent when proposed, and seemed to be aimed at ensuring the security service would be able to undertake illegal and unconstitutional activities. It was shameful that this measure was passed by a democratically elected parliament, and that shame continues as long as it is in effect.

The Constitution is the supreme law of the land, and all government activities are required to be compliant with the Charter. Sadly, we have had decades of activities by the security services going back to the RCMP Security Services which were the subject of the MacDonald inquiry

where illegal activities appear to be standard operating procedure.

This is why stringent and independent oversight is required.

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?**

The problem is the unsubstantiated power to share large amounts of personal information on a very low standard. The *SCISA* should be repealed.

The large scope of other activities that are set out as undermining the security of Canada include activities have little or nothing to do with terrorism, and will almost inevitably result in legitimate dissent or protest being targeted.

- **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?**

Repeal is required, not tinkering.

- **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?**

This is an example of either dishonesty or ignorance on the part of those who have put together this question. The Privacy Commissioner himself has explicitly stated earlier this year that his office is unable to provide review or oversight over the massive increase in data sharing created by C-51. Putting this forward as though such OPC review is actually possible or in fact taking place is designed to skew the responses toward a favourable reaction to a status quo that is already dysfunctional.

The OPC has put forward some useful suggestions if the government insists on maintaining this massive increase in surveillance of Canadians. Please see their response to this consultation for details.

- **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?**

Once again, the Privacy Commissioner has explicitly stated that his office is not able to provide this type of oversight without additional resources. Regulations would be a band aid fix, when repeal is what is required.

- **Some individuals have questioned why some institutions are listed as potential recipients when their core duties do not relate to national security. This is because only part of their jurisdiction or responsibilities relate to national security. Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?**

The premise for this vast expansion of data mining on individuals on a rock bottom standard has never been fully articulated beyond 'it's just common' sense'.

What we have seen earlier this week from the Auditor General is that the government has no information whatsoever to show the large scale international information sharing with the United States as part of the Beyond the Border plan is in any way effective in achieving its stated goals.

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?**

Yes, if PPP is not abolished.

- **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?**

One way to reduce this phenomenon would be to allow those affected to sue for damages, including full rights of discovery of how their names were put on the list.

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

The appeals process would move much faster if there was a possibility of a lawsuit for damages including full discovery. It is unfair and unjust to require someone wrongly deprived of the right

of movement in a country as large as this to fight the government and security apparatus without having access to the basis of the decision making process.

SECTION 6: CRIMINAL CODE TERRORISM MEASURES

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

The reduction of the standard from 'likely' to carry out terrorist activity to 'may' has opened this measure to potential abuse.

Suspects are also required to answer questions posed by law enforcement when ordered by a judge, which turns our criminal justice system on its head.

In the aftermath of the Driver case, there are also some questions about the effectiveness of these measures.

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?

It is not a variation of counselling. If you are being advised to make this change in the hope it will better withstand a court challenge for infringing on constitutionally guaranteed rights of freedom of speech and of association, that is for you to determine.

Given the already voluminous list of terrorism-related offences, there is no obvious need for this.

- **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?**

This should be repealed in toto.

- **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?**

C 51 should be repealed. If the government is able to show that additional protections for national security witnesses are required beyond those already in the *Criminal Code* and elsewhere, they should bring forward a bill dealing this this.

SECTION 7: PROCEDURES FOR LISTING TERRORIST ENTITIES

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

The framing of this question is more suited to a request for advice to the Department of Justice than a public consultation. You should ask them for an opinion if this is in fact a question rather than a statement with a question mark.

- **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?**

The listing of groups can lead to negative consequences for individuals whose allegiance to such groups is tenuous especially if those groups were in physical control of a given area and able to exercise coercive power over those individuals.

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

Listing is essentially a shortcut for the security apparatus to categorize and deal with individuals without having to undertake detailed analysis or investigation of individual circumstances.

In 2003 the Hell's Angels were targeted in seizure of colours and other items at Montreal and Toronto airports, and police in Montreal openly discussed the possibility of listing the motorcycle gang as a terrorist organization under the then-new ATA. This shows the scope for potential abuse and/or overreach by authorities with large discretionary power.

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

Listed groups are placed in a very difficult position once that happens, and should have access to resources for the purpose of challenging that listing. This could be done on the same basis as for seizure of proceeds of crime under the *Criminal Code*, and the government should be required to back its listing with evidence.

SECTION 8: TERRORIST FINANCING

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

Please refer to the 2009 and 2013 reports by the Office of the Privacy Commissioner regarding FINTRAC for recommendations.

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

See above

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

See above.

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

See above.

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 Supreme Court of Canada and lower courts have made a number of decisions which this Green paper appears to take issue with. Rather than attempting to have these decision overturned legislatively, the government and security apparatus should concentrate on finding ways to do their job that are compliant with the law and Constitution.

- 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?

This is a false analogy, as the access to digital or electronic devices can reveal a great deal more than even entering into a dwelling.

Warrants must the tailored to the requirements of an actual investigation, rather than allowing a general ability to search a person's electronic devices.

- **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?**

Before anything is done in this sphere, the security apparatus must accept *Spencer* and other decisions regarding metadata. They have consistently claimed (as does this Green Paper) that that metadata is the equivalent of a phone book listing and is therefore not subject to a reasonable expectation of privacy.

That is not the case, as the Supreme Court set out in *Spencer*. Unless and until the government accepts the commonly understood interpretation of metadata and what it means for privacy, they should have their powers rolled back.

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

Read *Spencer*.

<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.**

It is unbecoming to try to undermine a recent decision of the Supreme Court of Canada protecting our personal privacy when CSIS and others have been shown to be so cavalier with collecting and using Canadians personal information.

- **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?**

This is another question designed to elicit a favourable response for the security apparatus based on false premises. Read *Spencer*.

- **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, and so does the Supreme Court of Canada.

Interception Capability

- **The Government has made previous attempts to enact interception capability legislation. This legislation would have required domestic communications service providers to create and maintain networks that would be technically capable of intercepting communications if a court order authorized the interception. These legislative proposals were controversial with Canadians. Some were concerned about privacy intrusions. As well, the Canadian communications industry was concerned about how such laws might affect it. Should Canada's laws help to ensure that consistent interception capabilities are available through domestic communications service provider networks when a court order authorizing interception is granted by the courts?**

With a warrant, this should be allowed. However, many Canadians have 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 two people suspected of planning or having committed a crime - not all the communications of one person or the other. 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.

It is worth pointing out that this question is misleading, as it suggests the police have no, or not enough, interception capabilities. However, 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 for lower-priority cases. Such economic rationales are one of the ways that society ensures police are circumspect in how broadly they engage in surveillance.

Encryption

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

The security and law enforcement agencies have been pushing consistently for backdoors to all types of devices. The net effect of this is to make anything with a backdoor less secure against malicious agents.

A new power for the authorities as set out in this question would violate the basic right against self-incrimination, and would likely be overturned by the courts.

- **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?**

See above. It appears the government and its agencies are willing to have all devices opened to malicious forces as long as they are able to have simple and direct access.

It is not possible to put a hole in what was a brick wall and then claim it is as secure as it was before.

<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?**

Preservation orders are already available with a warrant. A European blanket data retention directive was found to be contrary to European law, and it may well be that a similar law in this country would be unconstitutional for similar reasons.

- **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?**

It should not do this, see above.

SECTION 10: INTELLIGENCE AND EVIDENCE

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

No**.** Section 38 has also been used to cover up failure by Stingray cell phone interception devices in at least one case, as revealed by a Vice news story just out today.

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

As noted above in cases where damages are sought, counsel for the person implicated in this type of proceeding should have the ability to see the evidence in order to mount an adequate defence.

- **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?**

It is the lawyer representing the affected individual who should have access to the evidence.

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

See above

- **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?**

See above.

- **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?**

This entire system has been superimposed on the justice system. It does not work on the same basic principles as the criminal law in this country. To the extent there are any safeguards in place, they are designed to provide arguments against constitutional challenges rather than providing any real protections.

GENERAL FEEDBACK

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

See above regarding the integrated review body and related bodies. Parliamentary oversight should be by a parliamentary committee, not a 'committee of parliamentarians' under the thumb of the executive.

Finally, there need to be administrative consequences for those who have repeatedly undermined privacy rights through excessive and unwarranted surveillance. Even if these senior actors were not acting in bad faith, clearly their view of what is acceptable under the law of this country is startlingly different from the view of the courts, SIRC and most Canadians.

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

See above.

- **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?**

If anything, the government has too many unchecked powers in this area relative to what has been claimed to be the threat.

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

The government should consider the fact that this country has withstood a number of threats to its people and way of life, going all the way back to the Fenians.

We have overcome these threats using the criminal law and the protections it contains.

What the government and especially its security apparatus have been pushing for is the creation of a special class of offender, the terrorist, with special provisions that only apply to those put in this category.

This is a short-sighted strategy which only plays into the narrative of these groups. Rather than pursuing them using the criminal law for their criminal behaviour, the government's approach reinforces and confirms their narrative, which is that they are not murderers or extortionists, but freedom fighters who are being oppressed by the state. This can be very convincing, especially if the 'terrorists' are identified as coming from one group in society, which is turn makes cooperation harder to win among the wider population of that group.

We need to rely on our strengths as a society, not increase repressive powers to make up for our perceived weakness.

Please show a little more confidence in the people of Canada and the country we have built and maintained over the past 150 years.