National Security Consultations

What We Learned Report

Contents

1. Introduction

The National Security Consultations (the "Consultations") sought to engage Canadians, stakeholders and subject-matter experts on issues related to national security and the protection of rights and freedoms. The Consultations were held between September and December 2016 and covered a number of issues, including countering radicalization to violence, oversight and accountability, threat reduction and the *Anti-terrorism Act, 2015* (former Bill C-51). Input from the Consultations will be used by the government to inform the development of laws, policies and programs to ensure that the National Security Framework is effective in keeping Canada safe, consistent with societal values and aligned with the Canadian *Charter of Rights and Freedoms*.

Members of the general public were able to take part through a variety of forums:

- **Online Consultation on National Security:** With 58,933 responses, this generated the largest volume of input, using a questionnaire consisting of more than 60 open-ended questions, organized into 10 themes. In most cases, those who responded chose to focus on one or more specific themes or question(s).
- **Email Submissions:** This data source (17,862) consisted mainly of letters and other communications submitted by individuals. Many of the emails (17,373) came from co-ordinated online campaigns.
- **Public Town Halls:** Five town halls were held across Canada.
- **Engagement Events led by Members of Parliament:** Seventeen events took place at the constituency level and involved participation by members of the public. Some events also included experts and stakeholders.
- **Social/Digital Events:** There were two Twitter chats and one digital Town Hall event.

Two types of events were held to hear the views of academics and experts:

- Fourteen **in-person sessions** with academics and experts across Canada; and
- One **roundtable** with civil society experts.

Input from Organizations was obtained from 79 submissions from stakeholder organizations, experts and academics.

All data collected during the Consultations was assessed for quality, cleaned and prepared for analysis. Every comment, submission, letter and other input was carefully analysed. The results are summarized in 10 sections, one for each of the themes explored in "Our Security, Our Rights" National Security Green Paper, 2016 (the "Green Paper") and the online questionnaire:

- Accountability;
- Prevention;
- Threat Reduction;
- Domestic National Security Information Sharing;
- Criminal Code Terrorism Measures;
- The Passenger Protect Program;
- Procedures for Listing Terrorist Entities;
- Terrorist Financing;
- Investigative Capabilities in a Digital World; and
- Intelligence and Evidence.

For additional details on the data analysis, please see Appendix A.

2. Summary of Analysis

2.1. Overview of What We Learned

There is a delicate balance that must be struck between the secrecy and covertness in the fight against terrorism and the constitutionally protected rights and freedoms of individual Canadians. The secret and complex nature of much of the work done on national security matters and anti-terrorism activities means that, for many Canadians, their views on this issue come down to whether they believe governments, national security agencies and law enforcement need additional and potentially secretive powers to protect Canada's security and whether any existing or new powers are used in a way that does not unduly infringe on the Canadian *Charter of Rights and Freedoms*.

It is important to note, therefore, that public opinion research in Canada and elsewhere has shown a consistent decline over several years in the level of trust people have in a range of institutions, including the military, police, politicians, the media and the judiciary, all of which are relevant to the issues covered by the Consultations. This growing level of distrust in key institutions involved in national security and law enforcement was clearly evident throughout the Consultations.

Many individuals and organizations were skeptical of measures proposed in the Green Paper and expressed concerns about how these would affect individual rights and freedoms. Some participants rejected the need for new measures, and a majority of stakeholders and experts called for existing ones to be scaled back or repealed completely, particularly Bill C-51, the *Anti-terrorism Act, 2015*, with a number of roundtable participants saying that the National Security Framework should protect freedom of speech and protect against unlawful surveillance.

On the specific issue of a "No-Fly" list as provided for under the *Secure Air Travel Act* ("*SATA"*), online participants were generally supportive but wanted measures to reduce the number of false positives and an improved appeal process for anyone placed on the list, while most organizations and experts who expressed an opinion on the list questioned its effectiveness as a tool to prevent terrorism and wanted it either overhauled or eliminated.

Most of those who were prepared to accept some new measures and powers for law enforcement and national security agencies insisted there be additional oversight and transparency and more checks and balances. A clear majority of stakeholders considered current oversight to be inadequate, and many believe existing review bodies need more capacity and should be allowed to collaborate on reviews. There was strong support among roundtable participants and online responses for a single, expert, independent, non-partisan body to oversee all of the government's national security activities.

Many organizations and experts want further revision or reform of amendments to the *Criminal Code* in response to the *Anti-terrorism Act, 2015*, with many saying those amendments are unnecessary and should be repealed. Some organizations want a "sunset clause" or enhanced procedural safeguards for the new measures, and many called for more precise definitions of what constitutes a threat to national security and which activities should be exempt from scrutiny.

Government and police agencies want greater collaboration and information sharing as provided for under the *Security of Canada Information Sharing Act* ("*SCISA"*), but many other

stakeholders called for *SCISA* to be repealed or fundamentally revised, noting that existing review mechanisms do not provide sufficient accountability. A majority of responses, both online and in other forums, want *SCISA* to include a more precise definition of "activities of advocacy, protest, dissent and artistic expression" and greater clarity about what constitutes an "activity that undermines the security of Canada," as current definitions are considered too vague and could include activities that are actually lawful dissent or freedom of expression.

Throughout the Consultations, individuals and organizations emphasized the need to ensure an appropriate balance between ensuring national security and protecting personal privacy, with several non-governmental organizations concerned that the pendulum had swung too far toward security over privacy. Organizations and experts who took part in other forums also stressed the importance of safeguarding personal rights and freedoms but were somewhat more open to giving security authorities additional power and better tools. That said, most also called for better oversight of those authorities and for changes to legislation that would better clarify how those powers can be used and against whom. Furthermore, most of the participants who took part in the online consultations, as well as many experts and organizations, are reluctant to accept new powers and tools to enhance Canada's investigative capabilities in a digital world.

Another significant finding is that a clear majority of participants have an expectation of privacy in the digital world that is the same or higher than in the physical world. Many participants consider their activities online and on their computers to be "very personal" or "intimate" and a window into their inner selves. Unlike their life in the physical world – which has taken place over a lifetime, in different places, and in conversations that now only exist as memories – their digital lives are stored, organized and potentially accessible by others. Their concern to protect this information and their personal privacy goes well beyond fears about identity theft or Internet scams. As such, there was a consensus, including among organizations and experts, that law enforcement and national security agencies should act in accordance with the law and respect the Charter of Rights and Freedoms, whether in the physical or the digital world.

On balance, therefore, most participants in these Consultations have opted to err on the side of protecting individual rights and freedoms rather than granting additional powers to national security agencies and law enforcement, even with enhanced transparency and independent oversight. They also want the government to focus its efforts on preventing terrorism through measures to counter radicalization to violence, including through public awareness and education campaigns to promote diversity in Canada, better support for new immigrants and at-risk groups, and addressing root causes of radicalization by improving social programs dealing with such things as health (including mental health) and housing.

2.2. Key Findings by Theme

2.2.1. Accountability

Accountability was a central issue running through all sections of the Consultations and in all forums, with the vast majority of participants stressing the importance of ensuring that Canada's national security agencies are subjected to sufficient oversight to prevent unnecessary or excessive surveillance and protect Canadians' *Charter* rights and freedoms. Although there was unanimity on the need for oversight, views differed somewhat on whether it should be conducted by a government agency or an independent third party, the degree to which existing

review bodies should collaborate and share information, whether there should be a single reviewing body and whether any additional agencies should be subject to oversight and review.

Participants strongly supported giving existing review bodies – the Civilian Review and Complaints Commission (CRCC), which reviews the Royal Canadian Mounted Police (RCMP); the Security Intelligence Review Committee (SIRC), which reviews the Canadian Security Intelligence Service (CSIS); and the Office of the Communications Security Establishment Commissioner (OCSEC), which reviews the Communications Security Establishment (CSE) – greater capacity to review and investigate complaints against their respective agencies. Two-thirds (67%) of online responses and a clear majority of stakeholders favoured increased capacity for the review bodies, but one in five online responses said the existing bodies can never provide adequate oversight, with most citing a need for independent or third-party reviews instead.

Most online responses provided little or no rationale to support increasing the capacity of the review bodies, but some of the reasons that were given included allowing the review bodies to compel testimony or to have the ability to act upon their recommendations by taking corrective action. Some responses also called for more resources and funding to improve review mechanisms.

There was also strong support for allowing the existing review bodies to collaborate on reviews, with 72 per cent of online responses and a majority of stakeholders favouring increased collaboration, but 15 per cent of online responses opposed the idea, usually citing the need to keep the review bodies independent of each other. Some also felt that there are too many review bodies, suggesting there could be merit in streamlining or consolidating the process.

Among the reasons cited for increased collaboration was a general sense that it would enhance review mechanisms and a belief that, if the security agencies are allowed to collaborate, so too should the bodies that review their activities. Some responses said there should be additional oversight of any collaboration, perhaps through judicial review.

Four-fifths (81%) of online responses want independent review mechanisms for other departments and agencies that have national security responsibilities, such as the Canada Border Services Agency (CBSA) and the Canada Revenue Agency (CRA). But 13 per cent oppose the idea, preferring to maintain the focus on current review mechanisms and because additional oversight could reduce the effectiveness of the agencies.

Despite the broad mandate of the proposed Committee of Parliamentarians to examine the national security and intelligence activities of all departments and agencies, three-quarters (77%) of online responses believe there is a need for an independent review, as recommended by Commissioner O'Connor, some suggesting the creation of a "super" review body to consolidate all oversight functions now conducted by CRCC, SIRC and OCSEC. Most responses suggested such a review could complement the proposed Committee of Parliamentarians while others said the committee lacks the necessary expertise to conduct such reviews, a view shared by many roundtable participants, who felt parliamentarians would need support from experts who could provide independent advice. Those participants preferred the establishment of a Committee of Parliamentarians accountable to Parliament, not to the Prime Minister, a view echoed by some participants in the public consultations held by MPs with their constituents.

There was strong support among roundtable participants and people who attended Town Hall consultations for a single expert, independent, non-partisan body or an Officer of Parliament with responsibility for national security, akin to the Auditor-General.

Very few online responses suggested additional measures to increase parliamentary accountability for the *Anti-Terrorism Act*, 2015 ("*ATA, 2015"*) beyond the promised statutory review of the legislation after three years. At MPs' forums, however, a majority of participants thought the Committee of Parliamentarians on National Security and Intelligence would improve the accountability of the national security agencies. Several email submissions called for any legislation that impacts privacy to be subjected to regular review.

2.2.2. Prevention

Preventing radicalization, particularly of youth and marginalized populations, was seen as an important goal of the government's National Security Framework. Participants believe that addressing the root causes of radicalization, particularly its social and economic determinants, should be a priority focus, with both short-term, practical action that emphasizes prevention through screening and policing and a longer-term strategy that engages communities in meaningful programs to deal with root causes at the local level. As there is no "one size fits all" solution, government should work closely with communities to develop solutions for each specific situation and location.

Participants generally saw government as having three main roles in preventing radicalization: as a funding body, particularly of community programs and awareness campaigns; as a policy maker, notably in the areas of immigration screening, criminal sanctions and improving social and economic conditions for at-risk communities; and as an co-ordinator, facilitating greater collaboration among federal departments and with other levels of government.

Many participants said Canada should review its foreign policy positions and role in the Middle East, with an emphasis on increased peacekeeping initiatives that would improve Canada's reputation abroad and reduce the terrorist threats it faces. Several participants also want more effective settlement programs for new immigrants that would help them integrate into their communities, and an enhanced screening process to deter "at-risk" individuals from entering Canada.

Community engagement was seen by many as a high priority, with an emphasis on youth in order to counter radicalization at an early age. A clear majority of stakeholders and experts supported the Green Paper's acknowledgement of the need to collaborate with communities on grassroots activities, with some participants also calling for a focus on engaging the wider Muslim community, as well as women, new immigrants and impoverished communities, as all of these groups can be vulnerable to social isolation. These engagement activities should be accompanied by public awareness campaigns that promote available community programs and alternative narratives. Coupled with calls for specific actions, there was also support for addressing factors that contribute to radicalization, such as poverty, health (including mental health) and housing, and a general agreement among stakeholders on the need to create a counter-narrative and mobilize positive content that diminishes anti-Islamic language and Islamophobia.

In contrast to those advocating “soft” actions, other participants took the view that security should be paramount, calling for increased intelligence gathering and surveillance capabilities, increased criminal sanctions and revised immigration policies and tougher screening.

Understanding the causes of radicalization to violence was seen by many as the top priority for additional research, followed by examining counter-radicalization and rehabilitations efforts, and the impacts of social and digital media, but one in five online responses thought research funds would be better spent on measures such as public awareness campaigns or improved health and social services.

2.2.3. Threat Reduction

This section of the Consultations looked at CSIS’s threat reduction mandate, including its original powers to collect information and advise law-enforcement agencies about suspected threats to the security of Canada and its new powers under Bill C-51 (*ATA, 2015*) to take direct action to reduce those threats. While online responses were essentially divided between the need to decrease CSIS’s powers and the need to maintain or increase them, many participants in other forums favoured reducing them and returning CSIS to an information gathering agency, citing serious concerns about the potential impact of its new role on rights and freedoms.

Among those who wanted to curtail CSIS’s powers or eliminate the agency altogether, most cited their lack of trust in national security agencies and their concerns about protecting personal privacy. Even those who felt CSIS’s powers are sufficient or should be increased thought there should be more information sharing with other security agencies and departments, greater transparency and more oversight to prevent abuses of power and to improve public support.

It was widely felt that current safeguards around CSIS’s threat reduction powers are insufficient to ensure the agency acts responsibly and effectively. More than two-thirds of online responses called for increased safeguards, including greater oversight – preferably by a third party – to ensure that Canadians’ *Charter* rights and freedoms are always protected. An even higher percentage want Sec. 12.1(3) of the *Canadian Security Intelligence Service Act* amended to make it clear that CSIS warrants can never violate the *Charter*, while a minority oppose such an amendment because they believe that infringing *Charter* rights is acceptable when dealing with national security matters and CSIS should be trusted to safeguard the public interest.

Many participants in the in-person discussions and MP consultations had serious concerns with CSIS disruption activities and the potential for CSIS warrants to violate the *Charter of Rights and Freedoms*. This view was echoed by several organizations that made submissions to the Consultations, with a majority calling for the *ATA, 2015* to be repealed or amended because the government has not made the case for increasing CSIS’s powers nor shown that the increased scope will reduce threats to security. As in other forums, there was strong support for effective oversight mechanisms with sufficient resources to carry out their review mandate.

2.2.4. Information Sharing

Overall, a great deal of concern was expressed about the enhanced authority for national security information sharing among government institutions under the *Security of Canada Information Sharing Act* ("*SCISA"*) that was part of Bill C-51. Most participants believe oversight of *SCISA* should be strengthened to protect personal privacy and that institutions receiving security information should only use that information lawfully and in accordance with the rules that apply to those institutions. There is also widespread support for keeping detailed records of disclosure when sharing information and for reducing the number of government institutions that could potentially receive shared information to those with a core mandate for national security.

There was strong support among online responses (62%) and from participants who took part in other forums for *SCISA* to be further clarified by including a more precise definition of "activities of advocacy, protest, dissent and artistic expression" and greater clarity about what constitutes an "activity that undermines the security of Canada." Most participants felt that the current definitions are too vague and could cover activities that are actually lawful dissent or freedom of expression. But one in five (22%) online responses did not support clarifying *SCISA* because any anti-Canadian sentiments should be scrutinized for radical tendencies, including art and other forms of advocacy.

Most participants feel strongly that the government should make it clear in *SCISA* that institutions receiving national security information must only use that information as permitted by the laws that apply to them, including the *Privacy Act*. Many called for increased oversight and the imposition of penalties against any institution operating outside its existing mandate, but one in 10 online responses opposed clarifying *SCISA* as this could impede the work of law enforcement agencies.

Suggestions for increased oversight mechanisms included: an independent, third-party body; a unified or consolidated oversight body such as an Ombudsman to oversee all elements of the security apparatus; greater transparency and public access to information; routine, mandatory reviews; and increased powers for existing review bodies, including the Offices of the Privacy Commissioner and the Information Commissioner.

Three-quarters of online responses were in favour of new regulations to require institutions to keep a record of disclosure under *SCISA* to ensure proper accountability. Some responses went further, calling for individuals to be advised when information about them is shared. A minority of online responses (10%) opposed mandating records of disclosure as that could reduce the ability of departments and agencies to share information and could compromise the privacy of Canadians by making it easier for leaks or other losses of personal information to occur.

Many organizations recommended *SCISA* be repealed or fundamentally revised, with concerns – particularly among human rights, legal and community organizations – that the current definitions of information that can and cannot be shared are too vague and that existing review mechanisms do not provide enough accountability. Some pointed to the Maher Arar case as an example of how information sharing can lead to the deportation and torture of innocent people. Government and police organizations, on the other hand, supported greater collaboration and information sharing to protect national security.

2.2.5. Passenger Protect Program

While participants generally supported the need for a "No-Fly" list as provided for under the *Secure Air Travel Act* ("*SATA"*) that came into being with the passage of Bill C-51, there was a strong consensus that measures are needed to reduce the number of false positives and to improve the appeal process for anyone placed on the list. Many participants also want individuals to be notified if they are put on the list and to be given the reasons for their inclusion.

A majority of responses in both the online consultations and other forums want the Minister of Public Safety and Emergency Preparedness, who is responsible for *SATA*, to be required to decide within 90 days on any application by an individual to have his or her name removed from the list. In their view, 90 days is more than adequate and any longer would be an infringement on the individual's rights. But just over a quarter (28%) of online responses believe the Minister should be given even more time to make a decision, as removing names without proper clearance poses too high a security risk.

Many online and stakeholder responses called for speeding up the process for dealing with false positives, with suggestions that included making the list public and requiring more identifying information (such as passport number, photo ID or biometric scanner) than just a person's name. This was a priority theme at some of the MP consultations, with some participants from the Muslim community expressing their fear that they could be unable to return to Canada if travelling abroad and confused with someone who has a similar name to theirs. Several participants who attended Town Hall consultations spoke about their own experiences with the "No-Fly" list, or those of their families or friends, including their inability to convince authorities they had been listed unfairly or confused with someone else.

Most organizations representing civil liberties, legal, human rights, labour and cultural groups that took part in the Consultations challenged whether the "No-Fly List" is effective in preventing terrorism, with some of them questioning the constitutionality of *SATA* on the grounds of racial profiling. Many called for improvements to prevent false positives and a clear process for the expeditious removal of Canadians from the U.S. "No-Fly" list or to prevent Canadian airlines using the U.S. list. One in five (22%) online responses called for the *SATA* list to be abolished because it is ineffective and violates individual rights.

2.2.6. *Criminal Code* Terrorism Measures

A majority of Consultation participants expressed concerns about amendments made to the *Criminal Code* in response to the introduction of the *Anti-terrorism Act*, *2015*, particularly the risk that these amendments could lead to a loss of personal liberties and infringe on freedom of expression. There is concern that the new measures make it easier for authorities to detain or restrict people who have not been charged with or convicted of an offence, and that changes made to the requirements for obtaining recognizance with conditions or terrorism peace bonds, as well as changes to advocacy offences, are now too vague and open to subjective interpretation so that innocent people will now face greater harassment.

That said, participants are divided on whether the amendments should be repealed, modified or retained, although most organizations providing comments said the amendments were

unnecessary and should be repealed, while many email responses called for the complete repeal of provisions of the *ATA, 2015* "criminalizing free expression."

Among online responses, while 30 per cent think the thresholds for obtaining recognizance with conditions and terrorism peace bonds are appropriate and strike the correct balance between national security and protecting the rights of individuals, two-thirds think they are not – with roughly one in four of those participants thinking that the thresholds are too high and hinder protecting national security and the rest thinking they are too low and open to potential abuse. Many organizations providing comments to the Consultations said the amendments to the *Criminal Code* were unnecessary and should be repealed, and the previous legal thresholds reinstated. Some organizations said there should be a "sunset clause" or enhanced procedural safeguards for these *Criminal Code* amendments.

While almost half (47%) of online responses say the advocacy offence should be clarified so that it more clearly resembles the existing offence of counselling, almost one quarter (23%) disagree and one in five (21%) think the *ATA, 2015* should be repealed in its entirety or that sections of the *Criminal Code* regarding advocating and promoting the commission of terrorism should be repealed. When asked whether "part of the definition of terrorist propaganda referring to advocacy or promotion of terrorism offences in general (should) be removed from the definition," the divide is even closer, with 40 per cent in favour, 43 per cent opposed and nine per cent preferring that it be clarified to make it less broad in scope. Most organizations said the definition is now too broad and could lead to the conviction of innocent people. Many also questioned whether the advocacy offence is necessary given that "counselling" is already a terrorism offence under the *Criminal Code* and called for the repeal of sections of *ATA, 2015* dealing with the seizure and deletion of "terrorist propaganda."

Roughly one third (32%) of online responses do not see the need to change the protections given to witnesses and other people in the justice system under *ATA, 2015*, one in six (17%) don't know and the rest want to see, among other things, improvements to protect the anonymity of witnesses, the right for defendants to see their accusers and compensation for those wrongly accused.

2.2.7. Listing Terrorist Entities

Compared to other themes examined in the Consultations, this one tended to generate less feedback, with the responses that were received suggesting a certain amount of collective ambivalence. Online responses were roughly evenly divided between those that thought the current listing methods meet Canada's domestic needs and international obligations (52%) and those who thought they did not (44%), with neither side providing much explanation for their position. This theme also did not elicit many responses in the other forums, although some organizations – among them legal, human rights and journalism organizations – said the methods are too broad and largely ineffective.

Some of the online responses said listing known terrorist entities helps to reduce support for those entities and prevent acts of terrorism, but others believe that "terrorist activity" is either undefined or too broadly defined, allowing too many groups or individuals to be listed. Some responses said the list should be abolished completely because of the arbitrary nature of the

selection process and because those on the list lose privacy and other rights without proper due process.

Views were equally divided about which groups should be the focus of listing in future. One quarter (24%) of online responses said the focus should be on known terrorist entities, followed by: any organization that advocates violence to achieve specific outcomes (17%); any citizen affiliated with a terrorist entity (15%); any group or individual that threatens the security of Canada (14%); potential terrorists (12%); and anyone who financially supports a terrorist organization (8%). Roughly one in six (16%) of online responses saw no need to change the current focus, and a similar percentage thought no one should be the focus and the list should be abolished because it is ineffective at reducing terrorism threats, undemocratic and infringes on the rights and freedoms of individuals

Those who did not call for the abolition of the list had diverse views on what could be done to improve its efficiency, ranging from making the list and the criteria used to place individuals and groups on it public (26%), sharing the list with domestic and foreign agencies (11%), frequently updating the list (10%), removing the political role of ministers in order to avoid conflicts of interest (10%), and following judicial process (2%). About one in eight online responses (13%) said no changes are needed, while one in 10 called for abolishing the list, with some saying the terrorist threat in Canada is either overblown or non-existent.

A majority of online responses (62%) said current safeguards do not provide an adequate balance between national security and protecting the rights of Canadians and offered several suggestions for improving the safeguards, ranging from clarifying the definition of “terrorism” and the criteria for adding a group or individual to the list, making the list public, creating an appeal process and mandating more independent oversight. The other one-third of responses did consider the balance to be correct, but many of these respondents shared the view that “terrorism” could be better defined or clarified. Civil liberties and press freedom organizations called for additional safeguards against secrecy and cited the need for an appeals process.

2.2.8. Terrorist Financing

Consistent with views expressed in several other sections of these Consultations, most participants said that existing safeguards are insufficient to protect individual rights and those of Canadian businesses when tracking and blocking terrorist financing. They called on the government to implement policies and measures to strengthen public trust in the process, including increased oversight.

One-quarter of online responses (24%) said that no additional measures are needed to address terrorist financing, either because existing measures are adequate or because those measures are already too intrusive. Other responses offered suggestions on how to improve monitoring of terrorist financing, such as increased disclosure, more communication and sharing of information between the government and financial institutions, and greater use of newer technology. A number of responses said terrorist financing could be better deterred by freezing and seizing assets of terrorist groups or individuals, imposing sanctions against countries that shelter terrorist money and by imposing stiffer penalties on financial institutions that fail to report or that hide suspicious financing.

Nearly one-third of online responses (30%) emphasized that any measures designed to strengthen co-operation between the government and the private sector in preventing terrorist financing must maintain public trust in the process. This could be done by disclosing information to individuals and businesses when information has been accessed or shared, increasing the scope of regulatory bodies to oversee all information sharing and creating a more effective appeal process to challenge any restrictions placed on personal or business accounts.

Roughly one in five online responses (18%) want to see a more open dialogue between the government and financial institutions, including those that are unregulated, and greater information sharing. A similar percentage wants legislation to increase criminal and financial sanctions against private-sector businesses that do not report information about terrorist activity or suspicions about such activities.

Just over half (54%) of online responses said current safeguards are inadequate to protect individual rights and the interests of business, with many suggesting that existing safeguards allow for too much intrusion into private financial information and a smaller number saying those safeguards do not protect Canada from terrorist threats. One-third (34%) of responses were satisfied that existing safeguards adequately protected the rights of individuals and businesses.

When asked what changes could make counter-terrorist financing measures more effective while still respecting rights and protecting business interests, views among online participants were equally varied. The top suggestion, put forward by 36% of the responses to this question, was the need to encourage and strengthen public trust in Canada's security institutions, either through more oversight of government departments and agencies, including bodies such as the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), or the implementation of an appeals process, or both. Roughly one in eight (13%) responses called for increased monitoring of suspicious activity while slightly fewer (11%) thought increased co-operation between financial institutions to improve information sharing would enhance anti-terrorism procedures. A further 13 per cent said no changes are needed.

This section generated few comments from other forums, perhaps reflecting the complexity of the issues involved, but those organizations that did offer their thoughts were divided over whether any additional measures are needed. A few non-governmental organizations representing cultural and civil liberties organizations urged the government to implement suggestions made in 2009 and 2013 by the Privacy Commissioner regarding FINTRAC.

2.2.9. Investigative Capabilities in a Digital World

The need for new investigative capabilities to combat terrorism in a digital world was a major theme of the Consultations, drawing a majority of the feedback in the online forum (approximately 70% of total responses) and significant input from experts, organizations and others. Unlike many of the themes and specific questions covered in the Consultations – such as terrorist financing, terrorism peace bonds and defining terrorist propaganda and advocacy – digital surveillance and investigation was seen by most participants as having the greatest potential to directly impact their personal privacy, rights and freedoms.

It is not surprising, therefore, that participants emphasized that respect for privacy and due process are the most important considerations for national security agencies and law

enforcement when conducting investigations in the digital world. Many participants said that the challenges faced by investigators in the digital world do not justify circumventing existing rules and regulations and that, if anything, even more oversight and safeguard mechanisms are needed, given how often Canadians use the Internet for sensitive matters such as personal communications and banking. A clear majority of participants oppose giving government the capacity to intercept personal communications, even if a court authorizes the interception, and oppose any moves to weaken encryption technology. Even those who support broad powers of interception think it should only be allowed under rigorous judicial authorization and be limited in scope.

Perhaps the most revealing result of the online consultations is that seven in 10 responses consider their Basic Subscriber Information (BSI) – such as their name, home address, phone number and email address – to be as private as the actual contents of their emails, personal diary and their medical and financial records. Almost half (48%) said BSI should only be provided in "limited circumstances" and with judicial approval, and about one in six (17%) said it should only be available to law enforcement in emergency circumstances, and even then only with a judicial warrant. The principal concern about revealing someone's BSI is that it could be used for location tracking or to access even more online information about that person.

That said, there was a strong alternative view that law enforcement faces crucial delays and roadblocks that are impeding investigations, especially in the wake of the *Spencer* decision. Those participants who support this view say investigators need judicially authorized and timely access to this basic information, both online and on digital devices, to ensure authorities are best able to investigate criminal activity and keep Canadians safe.

Online responses also clearly (68%) supported the idea that law enforcement should operate the same in both the physical and the digital worlds, that privacy rights and due process needed to be respected in both, and that warrants issued for the digital world should be subject to the same level of scrutiny and consideration as they are in the physical world. There was also a consensus among organizations and experts that law enforcement should act the same in both the physical and digital worlds. Of the 28 per cent of online responses that said law enforcement should operate differently in the digital world, most said online data should require a higher threshold to be searched because of its personal and sensitive nature, with access granted only in the most perilous of circumstances.

Somewhat paradoxically, almost half (44%) of online responses said agencies should use the tools currently available as there is no demonstrable need for updated ones and giving investigators updated tools would only increase the power of investigative authorities to collect private data, install a backdoor on encryption or otherwise infringe on Canadians' rights. A further 41 per cent of online responses said law enforcement and national security agencies should have access to updated tools to conduct investigations in the digital world if they can demonstrate a need for them, but there was also support for adequate oversight to ensure these updated tools do not infringe on people's rights or privacy.

The vast majority of responses – more than four in five – show that the expectation of privacy in the digital world is the same as or higher than in the physical world. Some of the reasons given for a higher expectation of digital privacy are because people share many of their intimate and private thoughts online and use the Internet for sensitive activities such as banking and personal

communications. Some responses said they have a somewhat lower expectation of privacy online, particularly for content they post publicly, such as social media posts and comments.

In the area of increased authority and capabilities, nearly eight in 10 online responses (78%) oppose interception capability legislation and seven in 10 (69%) say there should be no consistent interception capabilities through domestic communications service providers, even if authorized by a court. In each case, the erosion of personal privacy was cited as the main reason for being against interception capabilities, with a secondary reason being the unfair burden this would place on service providers. Organizations that commented on these issues tended to argue against requiring providers to build interception capabilities into their networks, with many suggesting that some capabilities already exist and the government has not demonstrated a need for any changes. Many industry organizations said any increased costs of interception should be borne by the government.

Views were equally strong against giving investigators the ability to compel individuals or companies to assist with decryption. A clear majority of civil liberties, legal, academic and industry organizations whose submissions addressed this issue believe strong encryption is vital to protecting privacy and maintaining freedom of expression. Many organizations opposed “back doors” for law enforcement because they would weaken network security and leave them vulnerable to attack, with industry organizations stressing that encryption technologies are essential to promote trust in the system. Law enforcement said that, while the Framework should seek to maintain security for law-abiding citizens, it should also give authorities the tools they need to access the communications of those who use secure communications technologies for criminal purposes.

Most online responses (68%) opposed imposing a legal requirement on domestic communications service providers to keep telecommunications data for a specified period so it can be made available (with court authorization) to law enforcement and national security agencies to help with investigations. Of these responses, more than one third said retaining data could increase the risk of information being hacked or leaked inappropriately, while others said data retention could lead to abuses by the authorities. There were also concerns about the cost of storing so much data, pushing up prices for consumers and creating difficulties for smaller service providers.

Of the 28 per cent of online responses that supported some form of data retention, many said the legislation should be “reasonable” (such as covering only certain types of data and allowing deletion after a set period of time), require a court order or warrant for data to be released, and be subject to strict oversight. Most participants in this group thought retained data should be restricted to some forms of metadata and BSI, but they differed considerably on how long data should be preserved, with views ranging from less than a year (32%), between one and five years (8%), until an investigation is concluded (7%), between five and 10 years (6%), indefinitely (4%) or more than 10 years (2%). A further 37 per cent were less specific, with many preferring to leave it up to a court to decide an appropriate time period.

Among organizations who commented on this theme, most believe data retention should be limited to what is strictly necessary to meet specific law enforcement objectives and be subject to a specific retention order in each case. Law enforcement favoured a minimum retention period of at least six months. Email responses overwhelmingly opposed mandatory data

retention laws, while participants in the #YourNatlSec Twitter chat criticized the collection of metadata by CSIS and the government's overall record on protecting online privacy.

2.2.10. Intelligence and Evidence

This theme looked at the balance between the government's obligation to protect national security information and the use of that information in legal proceedings, including immigration hearings. Most participants said it is not possible to find an appropriate balance and that individual rights should always take precedence in courts of law as the non-disclosure of classified information can inhibit a fair trial. Many want more oversight and accountability when security information is not disclosed, are uncomfortable with the idea of in-camera proceedings and oppose the idea of having "security cleared lawyers" who can handle non-disclosed classified information.

Almost three-quarters (72%) of online responses believe the *Canada Evidence Act* should be amended to provide better protection of the rights of individuals on trial, increase transparency in the use of classified information in legal proceedings and give more power to judges overseeing cases. About one in five (18%), citing confidence in the judicial process, feel current measures are sufficiently balanced. Most of the organizations that commented on this section were legal or human rights groups, with the majority calling for reforms to Section 38 of the *Canada Evidence Act* to improve the balance between fairness and security.

Views among online participants were more closely divided on the issue of using security cleared lawyers in legal proceedings where national security information is involved, with half (51%) of responses accepting the need for such lawyers and a slightly smaller percentage (42%) opposing on the grounds that courts should remain "open," not "closed." Some organizations supported the use of security cleared lawyers, and some added that the special advocate should have access to all information in the possession of the government and be able to communicate with the named individual and the individual's legal counsel throughout the entire proceedings.

In the case of immigration proceedings, a majority (56%) of online responses believe that changes to Division 9 of the *Immigration and Refugee Protection Act* (IRPA) as a result of Bill C-51 do not have sufficient safeguards to protect individual rights, as defendants should be able to hear all of the evidence against them. They called for the end of closed court proceedings and the application of criminal legal procedures to all trials. About one in five (19%) of responses said the changes to the IRPA are appropriately balanced by safeguards, with some expressing the view that there are too many safeguards and that this could put public safety at risk. The few organizations that addressed this issue want the security certificate regime repealed because it is contrary to fundamental justice and the use of special advocates does not sufficiently compensate for this.

Appendix A

Analysis of the Online Questionnaire

The analysis of the online engagement questionnaire data was both quantitative and qualitative. The quantitative aspect was based on the systematic coding of the responses to questions. Both mutually exclusive and non-mutually exclusive coding categories were used, along with sub-codes where needed (i.e., to allow for a second, deeper level of analysis).

In cases where a consultation question asked for two pieces of information, they were usually treated as two separate questions, each with its own set of codes (e.g., “Should the SCISA be clearer about the requirements for listing potential recipients? Should the list of eligible recipients be reduced or expanded?”).

Each set of codes was empirically developed based on a review of large random sample responses (n=300 to 1,000). That is, based on the data itself, as opposed to a preconceived hypothetical range of anticipated responses. The objective was to create codes that are at once reflective of Canadians’ input, as well as helpful to the development of a national security framework.

Questions that could be responded to in the affirmative or negative, or for which it was highly unlikely that one would provide a range of views or suggestions, were given mutually exclusive codes (e.g., “Do the current Section 38 procedures of the Canada *Evidence Act* properly balance fairness with security in legal proceedings?”). Other questions, such as those that ask for suggestions, were given non-mutually exclusive codes (e.g., “Do you have any additional ideas or comments on the topics raised in this Green Paper and in the background document?”). In all cases, the coding framework also allowed analysts to distinguish between “don’t know,” “other” and “no response.”

Further refinements to the coding framework were made during the initial phase of coding (e.g., expanding codes, collapsing codes, creating new codes to reduce the proportion coded under “Other”).

The coding was done in Excel, with analysts selecting codes from drop down menus. Coded data files were transformed from Excel into SPSS to produce data tables of 1) overall results, and 2) cross-tabulations based on respondent profiling information (e.g., age, gender, region, etc.).

As part of the coding process, analysts made detailed notes (e.g., rationale for an opinion or idea) and selected verbatim representative quotes. The notes and quotes were used to qualitatively support and explain the quantitative results.

Email Submissions

The almost 18,000 email submissions were weighted heavily towards three advocacy campaigns that mobilized their supporters to communicate directly with government. The largest (Campaign A) accounted for 9,472 respondents, just over 53% of the total email submissions. The next largest (Campaign B) accounted for a further 7,415 emails, or almost 42% of submissions. Finally, the third largest (Campaign C) included 486 email submissions. Though it may seem insignificant when compared to the two larger campaigns, at just under 3% of the

total number of submissions by Campaign C still represents over half of the email submissions that do not fall into either Campaigns A or B.

The campaigns differed slightly in their approaches for communicating their key messaging. Campaigns A and C urged their supporters to echo their choice of wording exactly, simplifying the desired message. Alternatively, Campaign B provided respondents with a choice of prepared options for key recommendations, organized along the themes outlined in the Green Paper from which to build their submissions.

Of the email submissions that did not belong to one of the three advocacy campaigns, 25% were Newsletters or other automated content, 23% were submissions from organizations that shared an attachment, 9% were requests for additional information regarding the public consultations, and 8% shared no relevant information or recommendations. The remaining individual email submissions were considered and analyzed along the same thematic lines outlined in the Green Paper.

Analysis of the Data Generated by the Other Consultation Methods

The analysis of the data produced by roundtables, town halls, and other in-person events was qualitative. Guided by Grounded Theory[1], content analysis matrices were developed for each data source/method of engagement and organized according to the main consultation themes.

Each set of notes, synthesis report, submission and email was analyzed and disaggregated with each significant point or comment inserted under each theme as appropriate, along with verbatim quotes and source identifier (e.g., “Halifax Public Town Hall”). Once the analysis was complete, the matrices allowed us to identify key points of convergence and divergence.

[1] Glaser, Barney G. and Strauss, Anslem L., The Discovery of Grounded Theory, Strategies for Qualitative Research. Aldine Transaction, New Brunswick New Jersey, 1967.