Canada and the 'Five Eyes' Alliance: Current directions in domestic national security policies

by

Julianna Mitchell

B.A. (Criminology), Vancouver Island University, 2014

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Arts

in the
School of Criminology
Faculty of Arts and Social Sciences

SIMON FRASER UNIVERSITY
FALL 2018

Approval

Name:	**Julianna, Mitchell**
Degree:	**Master of Arts**
Title:	**Canada and the 'Five Eyes' Alliance:** **Current directions in domestic national security policies**
Examining Committee:	**Chair:** Sheri Fabian Senior Lecturer
	Garth Davies Senior Supervisor Associate Professor
	Bill Glackman Supervisor Professor
	Raymond Corrado Supervisor Professor
	Bob Young External Examiner Director General, Canadian Security Intelligence Service, BC and Yukon - Retired
Date Defended/Approved:	November 13, 2018

Abstract

On June 18, 2015, the Canadian government passed the *Anti-terrorism Act (ATA)* with the purpose of enhancing Canada's national security strategy. The *ATA* has faced extensive criticism with many questioning the legality and necessity of the government's approach to domestic national security. However, little attention has focused on how Canada's national security measures compare to strategies implemented by other democratic nations. A comparative policy analysis is utilized to systematically examine some of the most controversial measures contained within the *ATA* in comparison to equivalent legislation existing among member-states of the 'Five Eyes' alliance. Relevant insights into the development of national security policies and practices are generated along with recommendations to improve Canada's current national security framework.

Keywords: *Anti-terrorism Act*; Canada; Five Eyes; national security; countering domestic terrorism

Dedication

This thesis is dedicated to my late Grandma Elizabeth Mitchell. I love and admire you to no end.

Acknowledgements

I am grateful to many individuals who played a substantial role in helping me arrive at this point. First and foremost, I am tremendously thankful for having the opportunity to learn from and work with my senior supervisor Dr. Garth Davies. I am indebted to you for your incredible mentorship and unrelenting support over the past several years.

I would also like to thank the other members of my supervisory committee. Dr. Ray Corrado and Dr. Bill Glackman, I am profoundly grateful to have had you both on my committee. Your feedback and direction were so appreciated, and contributed to the improvement of this thesis. Thank you both. I would like to extend a special thank you to Mr. Bob Young for being my external examiner. Your perspective and practical insight were invaluable. Finally, thank you to Dr. Sheri Fabian for chairing my defense.

Thank you to my friends in graduate school; this process would not have been the same without you and your support. I couldn't have asked for a better group to spend long days and nights reviewing stats with.

To my friends, thank you so much for your encouragement and support. In particular, thank you to Leah and Savannah; words cannot express how grateful I am for your friendship, love, and laughter.

Finally, thank you to my incredibly supportive family. Mom, you are my inspiration and my rock. Thank you for always being there to listen and guide me through any obstacles. Dad, I could not have done this without your motivation and unconditional support.

Table of Contents

List of Acronyms

ATA	*Anti-Terrorism Act, 2015*
Bill C-59	*An Act Respecting National Security Measures, 2017*
PP	Canadian Passenger Protect Program, 2007
Charter	*Canadian Charter of Rights and Freedoms, 1982*
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
CSIS Act	*Canadian Security Intelligence Service Act, 1985*
NAFTA	North American Free Trade Agreement
NATO	North Atlantic Treaty Organization
NSIRA	National Security Intelligence and Review Agency
NSS	National Security Strategy
PATRIOT Act	*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*
SATA	*Secure Air Travel Act, 2015*
SCISA	*Security of Canada Information Sharing Act, 2015*
SIRC	Security Intelligence Review Committee
UK	United Kingdom
US	United States
9/11	September 11, 2001

Chapter 1.

Introduction

Over the last two decades, concern over terrorist-related activity and homegrown terrorism has increased on a global scale (Freese, 2014). As a result, there has been a proliferation of government action aimed towards countering terrorist-related threats in the form of national security legislation, policies, and programs. The United Nations has deemed terrorism a chief concern in their global agenda, urging member countries to develop comprehensive strategies to combat terrorism through individual and concerted efforts ("United Nations Action to Counter Terrorism," n.d.). There appears to be an overwhelming consensus that no nation is sheltered from acts of terrorism. As such, national security has become paramount for many national legislatures. This new environment of heightened security has resulted in the swift adoption of extensive and draconian security laws in many countries (Kossowka, Trejtowicz, de Lemus, Bukowski, Van Hiel, & Goodwin, 2011; Roach, 2011).

National security legislation has consequently become an ongoing challenge for government; changes are often highly scrutinized and attract polarizing views from the public. A largely binary perspective on these policies has emerged, where some argue the scope and intensity of national security measures have dramatically and disproportionately increased as a consequence of terrorist incidents in the 21st century (Mueller & Stewart, 2012) and others posit that such tough measures are necessary to protect citizens and re-instill a sense of safety in society. As such, ample debate and controversy surrounds many of these measures and democratic governments face immense pressure to achieve a balance between implementing effective ways to prevent terrorist incidents while maintaining the public's rights and freedoms. The occurrence of terrorist events undeniably threatens society's collective sense of public safety and, consequently, societal attention turns to governments for protection. At the same time, society also expects that such measures will not derogate constitutional rights. This creates a complex balancing act for governments - how can they craft legislation that affords them the power necessary to prevent terrorist acts while continuing to protect their citizens' rights and freedoms?

Scrutiny of government action is necessary, as responses to terrorist events can have significant and long-lasting impacts on society, both nationally and internationally. A case in point is the US government's swift implementation of the *PATRIOT Act* in response to the 9/11 attacks. While this piece of legislation was deemed necessary by the government to restore public safety and thwart any further terrorist attacks, it also fundamentally changed the conception of privacy rights in the US by introducing measures such as roving wiretaps, the ability to collect "tangible things" on any "relevant" matters to counter-terrorism, and allowing the FBI to covertly search homes and businesses with delayed notification to the targeted individual(s). As such, the *PATRIOT Act* revolutionized the powers of the US government in relation to collecting intelligence and conducting surveillance. After the initial trauma of 9/11 subsided it became clear that these legislative powers had an extremely harmful effect on how individuals viewed their privacy and security – not only in the US but globally. This was magnified with the 2013 Snowden revelations.

The effects of the *PATRIOT Act* continue to permeate discussions of government authority and legislative latitude. In November 2017, the International Criminal Court announced an investigation into allegations of war crimes by the US Military and CIA in Afghanistan over 2003-2004. Such allegations included the use of "enhanced interrogation tactics" that were authorized by the *PATRIOT Act.* These tactics are alleged to have included torture and cruel treatment of detainees in detention facilities with the purpose of obtaining intelligence on suspected terrorists following the 9/11 attacks (The Associated Press, 2017). While this investigation will focus on the actions of the US Military, Canada and other US allies may also feel the ramifications. Indeed, although Canada and other US allies did not participate in such acts or condone the use of torture, each of these countries' spy agencies worked closely with their American counterparts during this period and heavily relied on American intelligence. The Canadian Security Intelligence Service had liaison officers working in CIA headquarters during this period, and vice versa (The Associated Press, 2017). As such, many have argued that Canadian and allied intelligence agencies were aware of, or at least suspected, how this intelligence was generated and are thus culpable for the heinous acts committed (Mayer, 2014). Additionally, increased intelligence sharing between Canada and the US post-9/11 has led to other cases of torture and clear violations of human rights, such as those involving Canadian citizens Maher Arar and Omar Khadr.

As these cases highlight, increased national security measures, while seemingly necessary to preserve public order, can have significant impacts both nationally and internationally and result in severe human rights violations.

Due to the highly controversial nature and lasting impacts of national security and intelligence practices, it is imperative that governments strive to create policies that find the right balance between effectively securing public safety through the prevention and deterrence of terrorist threats and protecting citizens' rights and freedoms. Robust national security measures are necessary to aid the prevention of terrorist or extremist attacks and limit their consequences. Such measures enable government to maintain public order and allow national forces to more effectively manage threats. Yet, democratic governments are also responsible for ensuring they act within legal parameters and respect citizens constitutional rights. Absent this, citizens will not have confidence and trust in government action (Diamond, 2007). This would make it impossible to employ effective governance and maintain public support in a democratic society. Since 9/11, Canada has continued to make changes to its national security framework in an attempt to achieve this delicate balance, most recently in the *Anti-terrorism Act* ("*ATA*"), 2015, and now through potential changes introduced in Bill C-59: An Act respecting national security measures (2017).

Since the inception of the ATA in 2015, criticism over the scope of the government's authority has riddled this piece of legislation and led to widespread skepticism of the changes it introduced (Roach & Forcese, 2015a, National Security Consultation, 2017). The 2015 ATA in Canada was brought in by the Conservative Government under Prime Minister Stephen Harper with the aim of strengthening and protecting Canadian society against "activities that undermine the security of Canada" (*ATA,* 2015). However, the unprecedented expansion of government power was widely criticized because it risked undermining Canadian civil liberties and negatively affecting the security of Canada (Roach & Forcese, 2015a).

The ATA became a focal point during the federal election in 2015. While the Conservative party maintained the necessity of the ATA, the Liberal party ran on the promise of reforming the ATA to resolve its issues (Public Safety Canada, 2017). After the Liberal government was elected in late 2015, it embarked on a series of consultation meetings across Canada between September-December 2016. These consultations

culminated in the publishing of “National Security Consultation: What we Learned Report” which guided the Liberal’s creation of Bill C-59 (Public Safety Canada, 2017; Bill C-59, 2017). The main purpose of this legislation is to limit some of the controversial powers outlined in the ATA. While this Bill has not yet been formally enacted, this is likely to occur in 2018. The Liberals state that their primary goal in introducing the legislation was to better strike a balance between rights and freedoms.

Despite this new legislation, divergent perspectives among government figures and citizens remain regarding what should be the look of Canada’s national security framework. Some argue that the limiting provisions of ATA go too far and impede the ability of Canadian security forces to protect society, while others maintain the new limitations don’t go far enough and what remains of the ATA still unduly encroaches on citizens’ rights and freedoms. Meanwhile, a myriad of terrorism acts continues to shock democratic societies. Such occurrences rekindle public calls for government to prevent these types of incidents. Terrorist attacks at concerts in Manchester and Paris, and via automobiles in New York, Nice and Barcelona, demonstrate that Canada and other Western countries are not immune from such attacks. As such, there remain contentious opinions on how far-reaching national security measures should be, leaving policymakers grappling with crafting national security strategies that both effectively protect national security and respect citizens’ rights and freedoms (Sample, 2008).

While much discussion has focused on the expansion of powers and new measures contained in the ATA, little attention has focused on how this framework compares to the national security strategies developed by other nations. Additionally, how Canada’s perceptions of national security threats equate to those held by allied countries also has been largely unexplored. National security perceptions shape national responses to security governance, including how to prevent, protect, and deter terrorism or extremism and ensure public safety.

1.1. Current Study

Accordingly, this research aims to systematically review and compare Canada’s current national security framework to legislation employed by allied democratic countries. The focus of this comparative policy analysis will be on domestic national security provisions implemented by members of the Five Eyes alliance. Members of the

Five Eyes alliance include: Canada, the United States of America ("US"), United Kingdom ("UK"), Australia, and New Zealand. This analysis is confined to these countries as they share common legal and political heritage; these structural similarities allow for more informed comparisons across different countries and national contexts. Additionally, these countries form the cooperative intelligence-sharing Five Eyes network that gives these countries a unique bond when it comes to national security. Each country's national security measures are examined following a similar template and a comparative approach is used to disentangle varying national security approaches.

The analysis will examine security practices in the wake of national and international terrorist events, and evaluate divergent government responses on national security. These practices will then be evaluated to contextualize how Canada's national security compares to foreign approaches and help inform principles that an effective national security framework should contain in the 21st century. Evaluating the similarities and differences between national security strategies crafted by democratic countries also provides an account of perceived security threats and the measures utilized in response, and advances insight into how each country balances national security and civil liberties. With these goals in mind, the analysis will first review theoretical frameworks and perspectives for understanding the different goals of domestic security legislation. Second, comparative case studies will be evaluated to understand the similarities and differences in Canada's national security framework approach. Finally, recommendations for improving the construction of national security strategies will be provided. Ultimately, this research aims to contribute to the ongoing reconceptualization of security in Canada and help policymakers strive towards a more effective national security model.

Chapter 2.

Policy Framework

National security has become a major topic of public, political, and legislative debate in democratic nations. Security-related issues have been regarded as among the most crucial responsibilities of government on both national and international levels, and resulted in governments crafting a wide spectrum of strategy-related documents. Domestic terrorist incidents have plagued governments worldwide and undermined their ability to assure public safety and show that these strategies can attain their objectives in preventing or intercepting threats. The events of 9/11 led legislatures to embark on quick and responsive action to address public concern. As such, national security strategies have been extended and supplemented to deal with perceived threats. However, the commitment to respecting citizens' fundamental rights when developing these strategies is an increasingly important and recognized task for democratic governments to maintain. A disregard for citizens' rights would erode support for government and their strategies (Diamond, 2007). The need to create enhanced security measures to combat national threats, while upholding citizens' rights and freedoms, has led to intense debate about if, or how far, these government measures can infringe on citizens' rights. The need to balance these competing interests has put immense pressure on governments and left them with a complex challenge: how do legislators endeavor to craft national security strategies that balance security and rights? The resolution to this question is complex and requires a consideration of changes in the national security landscape among global democratic nations.

National security strategies are intended to help guide governments with how to best protect the nation and its citizens; however, these strategies are difficult to craft and even harder to evaluate their effectiveness. To understand how these strategies are crafted and justified, it is important to review the concept of national security, purposes of national security strategies, and implications of national security strategies. Following this is discussion of what it means to pursue a "balance" between national security and civil liberty.

2.1. Conceptualizing National Security

The term ‘national security’ can be conceptualized in a variety of ways, with differing definitions across nations (Stolberg, 2012; Caudle, 2009; Golder & Williams, 2006; Demirsu, 2017). The reasons for these differences are diverse and are influenced by each nation’s political, societal, geographical, and economical state structures and interdependencies. National security is generally crafted as “a unifying document for the executive branch...designed to create an internal consensus on foreign, defence, diplomatic....economic, strategy” (Reilly, 2004) with the core function being to identify threats to security and craft measures to secure the safety of the nation and its citizens (Stolberg, 2012).

2.1.1. Purposes of National Security

There are a multitude of purposes a national security strategy should serve, such as: communicating strategic goals, the nation’s values, perceived threats to the nation and its citizens, delineating international and domestic considerations and trends, outlining challenges to attain stated objectives, determining courses of action and resources, providing guidance to government agencies, and as a tool for budget planning (Stolberg, 2012). However, a national security strategy should provide a resolute understanding of its overall purpose to citizens. Stolberg (2012) states that a nation’s security strategy should serve as a communication tool of the “grand strategy,” which Stolberg (2012) defines “is a conceptual framing that describes how the world is, envisions how it ought to be, and specifies a set of policies that can achieve that ordering” (p. 15). The strategy is meant to direct governments and guide the implementation of national security-related matters in accordance with the aims set forth by the grand strategy, including legislation, plans, programs, reports, and other activities. Each of these documents serves the security strategy and governments can justify policy or legislative changes by referring to the purposes of the “grand strategy”. Moreover, national security strategies are also utilized in the political realm, where various parties will put forth their own strategic vision to appeal to certain constituencies.

National security strategies provide insight into the security purposes of a nation by outlining how state actors seek to address threats; this also provides insight into a nation’s values. The threats identified and strategies employed can demonstrate a

nation's perception of what is in the national interest and how to best protect it. Johnson, Kartchner, & Larsen (2009) explained that the threats that nations seek to address through strategies convey a "strategic culture," which is a "set of shared beliefs, assumptions, and modes of behavior, derived from common experiences and accepted narratives (both oral and written) that shape collective identity and relationships to other groups, and which determine appropriate ends and means for achieved security objectives" (p. 4). It is this strategic culture that influences how government craft national security strategies. For this reason, it is crucial to consider a nation's national security strategies in addition to their specific policies and legislation. While policies merely outline which actions are being taken by the state, strategies go further by explaining *why* such actions are being taken. As such, examining a nation's security strategies provides us with important insights into its strategic culture. This demonstrates the values that governments believe must be protected and the measures they think are appropriate to do so.

2.1.2. Expanding Security: Traditional and Non-Traditional Drivers

Both the concept and purpose of security are fluid and can be influenced by a variety of nation-specific considerations. International events can also drastically influence the concept of national security. For example, 9/11 unsettled how many democratic nations perceived national security and initiated change in the concept and scope of national security (Caudle, 2009). Perceived drivers of national security have also broadened over the years to extend past traditional threats such as foreign powers or weapons or military conflict to that of non-traditional domestic security and transnational threats including disease, poverty, catastrophic disasters, climate change, stressors related to resource and energy, reliance on vulnerable critical infrastructures and weaknesses in respect of human rights (see Caudle, 2009, p. 11 for an extensive list of drivers).

Government approaches to national security and the measures they develop are largely based on what drivers they deem as threats to the nation as a whole and the priority that each threat is assigned. However, some argue that perceptions of security threats should be extended past traditional threats identified by government (Hoogensen & Rottem, 2004). For instance, Buzan, Waever and Wilde (1997) argue that non-traditional threats should be considered when crafting national security policy, including

issues of government legitimacy and authority of the nation, human agency and quality of life, and preservation of basic cultural values. Along with the consideration of non-traditional threats, Krause and Williams (1996) maintain that national security policy should also be driven by potential threats to an individual's rights, where national and individual citizen security are perceived to be of equal importance. As such, experts argue contemporary national security strategies need to unify both national and individual security interests to ensure the success of a society (Krause & Williams, 1996).

However, even if national and individual security interests or traditional and non-traditional threats are deemed to be an important part of creating a strategy, each democratic nation's merging of these drivers will invariably be unique. This can be seen when nations are facing imminent threats, as opposed to those that are not. For example, countries that have faced repeated domestic terrorist attacks, such as the UK, perceive growing extremism throughout the nation as one of the most important drivers of their strategy approach (Counter Extremism Project, 2017). Compare this with a country like New Zealand, which has had few terrorist attacks in its history, and which considers ecological issues to be of equal importance in their strategy.

And yet, if it is accepted that the national security strategy demonstrates a nation's overarching interests and perceived threats, and government is crafting these strategies, it begs the question of whether these strategies are truly reflective of the nation and its citizens' interests. Democratic governments have experienced much criticism from citizens over the national security strategies they have crafted and have been condemned for allegedly prioritizing security of the nation over individuals' fundamental rights and freedoms. To this point, a US citizen might argue that his right to freedom of privacy ought to be valued more than the theoretical threat of a terrorist act on US soil. Thus, while we can look to strategies to determine *what* values drive our national security policies, the question remains as to whether or not these are the correct values to protect. Indeed, many argue that enhanced government power, evident in legislation like the *PATRIOT Act,* disregard constitutional rights in favor of preventing domestic terrorist events (Forcese & Roach, 2015). This, it is argued, can undermine a nation's security because it erodes the fundamental pillars of democratic societies and promotes distrust of the government which, in turn, can foster domestic terrorism.

2.1.3. A Delicate Balance: Civil Liberties and National Security

There is an inherent tension between the measures necessary to maintain national security and the need to uphold constitutional values. This tension lies between the methods used to defend a nation while also protecting its citizens basic liberties. In a democratic nation, liberty is “considered to be the freedom to exercise one’s rights, and it should be provided by and protected by the state” (Warshawsky, p. 94, 2013). This often includes rights such as the right to privacy, the right to expression and speech, the right to religion, the right to conscience, and the right to protection under law and fair trial, among others. The balance between these fundamental liberties and national security is often at the forefront of debates when government introduces new security strategies or measures. At the core of this debate is whether the protection of fundamental rights and freedoms should always be maintained over the protection of national security (and vice versa) or if governments can navigate a way to “balance” these two.

Government powers used to protect national security is central to debates over security and liberty. The powers deemed necessary by government to defend the nation can have a cost to citizens rights, especially in regard to privacy. Many nations have been criticized for favouring national security over civil liberties including, to varying degrees, all Five Eyes members (Warshawsky, 2013). Governments have responded by pointing to the increase of domestic violence and terrorist incidents which have led to the re-evaluation of security measures. The argument put forth is that, in order to combat the changing nature of these threats, more intrusive approaches are necessary. These approaches could mean that liberties are infringed upon. True to this point, democratic governments have introduced waves of new legislation meant to address and respond to terrorism in the post 9/11 environment. Such legislation has provided police and intelligence agencies extended powers that limits citizens’ rights.

There are consequences to prioritizing one of these values over the other. Citizens’ rights and freedoms are considered to be among the pillars of a democratic society. If governments repeatedly or increasingly infringe on citizens’ basic rights, this can engender widespread distrust in society, and citizens may begin to withdraw from the political process or seek out more radical and extreme alternatives to follow. A complete lack of confidence and trust in government legitimacy thus produces a fragile environment where government cannot mobilize its citizens or work towards a vision to

strengthen the nation (Diamond, 2007). This can also result in citizens seeking out more radical alternatives to follow, and could foster domestic extremism. At the other end of the continuum, in times where a nation and its citizens are threatened, the state is responsible for ensuring measures are taken to address imminent danger. These measures may involve the limitation of rights where citizens must cede certain rights when necessary to keep the population safe from indiscriminate terrorist attacks (Golder & Williams, 2006; Lowe, 2014). Thus, experts argue that a balance between the interests of national security and civil liberty must be pursued – both are values for which the state has the responsibility to protect. Lowe (2014) emphasizes that when crafting national security strategies, legislatures must remember that security and liberty are not mutually exclusive values but rather inclusive.

Warshawsky (2013) suggests that a nation must take into consideration specific factors to pursue harmony between the two values. The first is that there must be a real and imminent threat to domestic security – where legislation is proportionately crafted to this threat. Quick responses made in fear, however, should be avoided, as this can produce legislation driven by emotion. Second, Warshawksy (2013) states it is critical that legislation is not drafted in perpetuity; instead, an end-date for legislation should be identified. If any civil liberties are infringed upon, there must be a clear date by which such infringement should cease. Additionally, it is argued that both the public and government need to remain vigilant. Pointing to public opinion polls, Warshawksy (2013) found that the public was willing to give up elements of freedom to secure domestic security following a terrorist incident. It is suggested that governments need to act responsibly and again not engage in emotional legislation or take advantage of public fear. At the same time, it is critical for the public to fight for their rights to ensure these democratic elements are protected. Lastly, it is argued that government must establish a system of checks and balances to ensure the protection of civil liberties.

It is imperative governments strive towards balancing strong national security measures and protected rights and freedoms. Each nation is guilty of having violated its citizens' rights throughout history. These violations of civil liberties, when done in the name of security, have caused widespread hardships that still resonate and haunt nations today. Additionally, such incidents can serve to undermine public confidence in government actions. That said, it is a vital government responsibility to ensure the nation and its citizens security. Such responsibility should require governments to take a

preventative approach and enact legislation that is proportionate to actual threats. With some restrictions on both security and liberty, it is possible, and indeed imperative, that national security strategies satisfy and protect both values.

2.1.4. Evaluating a National Security Strategy

As a first step in evaluating a nation's national security strategy and its values, one must assess the content and words of national-security related material. This can both directly and indirectly demonstrate how security is conceptualized, the threats and objectives identified, and the approaches for addressing such threats and achieving its goals. A specific lens will be used to assess the extent to which and how Canada and the other Five Eyes countries value and balance national security with civil liberties. By examining global national security policies, this thesis aims to contextualize Canada's national security approach among security perspectives and strategies deployed by democratic allied governments. The strategies reviewed will also provide insight into how these nations prioritize or balance national security measures and civil liberties, and recommendations will be provided on how Canada can achieve a national security framework that provides effective security measures and upholds the values of the nation. As discussed, this is an important consideration in creating successful and supported public policy in a democratic society.

Chapter 3.

Methodology

Comparative policy analysis can help identify patterns and themes in the process of policy making, formulation, implementation, and evaluation (Engeli & Allison, 2014). Existing open source literature on security strategies and legislation will be reviewed along with relevant primary source documents and online material to cross-verify information. A chief goal of this comparative policy analysis is to assess the similarities and differences, as well as emerging themes, between national security strategies employed in the Five Eyes community. Specific provisions of Canada's *ATA* and analogous measures adopted in the Five Eyes will also be reviewed. These specific provisions were chosen as they were at the forefront of Canadian political and public debate; some argued that these provisions violated fundamental rights and freedoms in favour of tough security measures. Following this comparison is a short overview of other nations' national security strategies, which will elucidate any important features of international practices that can provide additional insight into how national security is conceptualized and addressed by governments. Only strategies related to domestic measures will be reviewed; foreign security measures are not included in this analysis. All cases in this research have been examined in the period following 9/11 (2001) up to 2017 to assess the phenomenon of national security during this specific time. As previously discussed, the concept of national security and threats perceived by democratic nations changed drastically following 9/11 and resulted in sweeping legislative changes (Demirsu, 2017).

This comparative policy research design employs data triangulation to enhance the validity of the research. Data triangulation involves synthesizing and converging a variety of data sources to understand a concept, phenomenon, or situation within a study (Konecki, 2008). Qualitative discourse analysis has been criticized for being too subjective if based on single, unreliable sources of data (Demirsu, 2017), but data triangulation attentuates this critique by collecting and meshing different sources of data to make inferences about the phenomenon being studied. Evaluating various sources of data can reduce bias as it allows for careful consideration and investigation into potentially diverging and converging observations about a phenomenon to make

informed conclusions (Konecki, 2008). In this study, data triangulation is used to summarize and contextualize each country's national security strategy by comparing various sources of data, including: national security strategies, legislation, policies, government reports, scientific articles, and official declarations and speeches.

Based on the above method, a short overview of national security strategies employed in Canada, the US, the UK, Australia and New Zealand in the post 9/11 environment are first reviewed. Second, specific provisions of the *ATA* and similar measures employed by the other nations will be assessed with important comparisons and trends highlighted. Third, this analysis will evaluate to what extent these laws reconcile civil liberty and national security when crafting such measures. Relevant insights into the development of national security strategies will be generated, along with recommendations to improve and evaluate these strategies to better reach intended goals.

It is important to understand how Canada and other democratic countries perceive and respond to domestic security and threats, as these responses can impact the occurrence and changing nature of terrorism experienced by nations (Freese, 2014). Overall, the research findings can aid in the following matters: 1) providing insight into current governments' national security strategies and emerging trends across nations, 2) serving as a basis for establishing an effective national security framework, and 3) encouraging measures that appropriately balance national security and civil liberty within Canada.

Chapter 4.

National Security in Canada and the Five Eyes

In striving to be a leader in national security, Canada has maintained a cooperative and complex relationship with members of the Five Eyes, which also includes the US, UK, Australia, and New Zealand (Cox, 2012). This covert security and intelligence network took form in 1946 for the purpose of sharing intelligence (Cox, 2012). Historically, the Five Eyes members have each faced unique experiences with terrorism. These events have served as an impetus for policy developments to address distinct circumstances within each nation. However, it is apparent that these legislative changes, designed specifically for the home country, have had a significant influence on the strategies of other nations as well (Cox, 2012). This proposition is illustrated in the striking similarities throughout the Five Eyes' national security strategies (Roach, 2011). Past research has found that among these countries, there has been a particularly strong influence from US and UK legislation (Roach, 2011). Furthermore, there is mutual consensus among the Five Eyes that threats of terrorism cannot be fought unilaterally. Instead, terrorist-threats require a joint effort, with emphasis placed on attaining high levels of intelligence to inform action (McGill & Gray, 2012). To gain a comprehensive understanding of Canada's national security strategy and its stance within the international platform, it is imperative to examine how these interconnected democracies shape each other's legislative and policy responses to terrorism. As such, a policy-focused approach will be employed to foster a comprehensive understanding of security strategies and the overarching goals embraced in Canada, the US, the UK, Australia, and New Zealand.

4.1. Overview of Five Eyes National Security Approaches

This analysis will first introduce the national security strategies employed by governments in the US, UK, Australia, and New Zealand. The purpose is to first provide a short introduction to these strategies and a brief overview of important political or legislative changes. Second, specific measures enacted by the *ATA* will be compared to methods employed by these nations, highlighting similarities or differences. The four major provisions of the *ATA* evaluated in this research include: the addition of a

terrorism-related speech offence, the implementation of the *Security of Canada Information Sharing Act* (*SCISA)*, Canada's Passenger Protect program, and the expansion of the Canadian Security Intelligence Service's (CSIS) mandate and powers. These provisions were specifically chosen as the Canadian government argued that our allies already had these powers and that Canada was merely aligning itself with its allies; in contrast, critics fervently disagreed. These expanded measures prompted intense debate and were viewed as vastly magnifying government powers and potentially superseding citizens rights and freedoms. Each of these provisions is reviewed independently followed by a review of similar measures employed by the other Five Eyes. This will provide a basis from which to examine Canada's national security strategy and whether such measures can balance constitutional rights with the dictates of national security.

4.2. National Security Strategies Post 9/11

4.2.1. Canada: Changing the game or catching up?

Terrorist-related activity is not new to Canada; for example, the traumatic aftermath of Air India Flight 182 still resonates today, over 30 years later. Recent events, such as the foiled 2006 Toronto 18 plot, the 2014 Ottawa shooting on Parliament Hill, and the 2017 Quebec City mosque shootings, stunned Canadian society and warned them of the dangers associated with terrorism. These events, coupled with growing concern over foreign fighters and lone actors, led the previous Conservative federal government to enact a series of legislative and policy changes designed to strengthen national security (Public Safety, 2014). The *Anti-terrorism Act, 2015* is the most recently enacted legislation under this policy initiative.

Having received Royal Assent on June 18, 2015, the *ATA* delineated a series of changes and additional provisions that affected security, privacy, and the power of police and security agencies. The Conservative government that created and enacted the bill argued enhanced legislation was necessary to equip Canada with adequate legal tools to tackle the evolving threat of terrorism (Watters, 2015). The prevention of radicalization and recruitment was at the forefront of many of these discussions. Government officials contended the measures were both reasonable and proportionate, stating there can be "no liberty without security" (Watters, 2015). It was clear the Conservative perspective

was that if Canadian's security was not safeguarded, civil liberties would not be properly maintained. However, opponents maintained the provisions delineated within the *ATA* broadly and excessively expanded national security and diminished the rights and freedoms granted to Canadian citizens (Roach & Forcese, 2015a). Many pointed to the sweeping and harmful repercussions this type of government power had had in the US following similar expansions to government agencies power when it came to issues of national security.

Liberal government revisions - "Underway" but "on track"?

The *ATA,* although enacted, continued to be vigorously debated throughout the 2015 federal election campaign and became a polarizing issue throughout party leadership debates. The Conservative party maintained the newly enacted *ATA* provisions were necessary while the NDP was starkly opposed to the changes. The Liberal party took a middle stance on the issue, and ran on the promise that, if elected, they would keep the legislation but review certain "problematic" measures within the *Act* to address public and experts' concerns (Tunney, 2016). The Federal election resulted in Justin Trudeau's Liberal party forming a majority government in October 2015.

National Security Consultations

In September 2016, Public Safety Minister Ralph Goodale introduced "Our Security, Our Rights: National Security Greenpaper 2016" ("Greenpaper"). This document was created with the intention of prompting discussion among the public and experts, and focused on ten issues that the Liberals deemed to be the most contentious elements of the *ATA*, including: accountability, prevention, threat reduction, domestic national security information sharing, passenger protect program, Criminal Code terrorism measures, terrorist entity listing procedures, terrorist financing, investigative capabilities in a digital world, and intelligence and evidence (Public Safety Canada, 2016). The release of this document also prompted what the Liberal's called "National Security Consultations," which aimed to engage with Canadians, stakeholders, and experts across the country on the outlined issues between September and December 2016. The consultations took the form of online questionnaires, email submissions, public town halls, engagement events, in-person sessions with experts from a variety of backgrounds, and a roundtable with civil liberties experts. One of the main purposes of these consultations was to discuss the measures within the *ATA* 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" (*Public Safety Canada, 2017*).* The implementation of such consultations marked a stark difference in perspective between the former and new government. Whereas the previous government crafted these measures based on their perspectives of how government agencies can best enhance national security, the current government took a more open perspective – it was clear from the controversy of the *ATA* that Canadians wanted to have more of a role in determining how national security could best be achieved without derogating civil liberties. As previously discussed, public perceptions of the role of government are an important feature that shapes the latitude that governments have in creating and employing national security measures.

These consultations also focused on the themes discussed in the National Security Green Paper, 2016. The results highlighted that throughout the research, the majority of citizens had a distrusting attitude of government national security and law enforcement institutions and concerns over protecting their rights and freedoms. As discussed, distrust and lack of confidence in government institutions can be a significant impairment to establishing a supported national security framework. Many Canadians and experts opined that Canada's national security framework should be constructed in such a way that preserves citizens' rights and freedoms while granting national security and law enforcement agencies the power to effectively safeguard the nation against threats of terrorism. A main discussion point within the consultations was the rights of Canadians to have their personal privacy protected, especially in the digital realm. Many felt that, while it was important that government and law enforcement have the ability to conduct investigations in the online environment, it was just as important that individuals' privacy was respected with regard to their online activities and personal data. To this point, an overwhelming majority of participants felt that digital surveillance and investigation has the greatest potential to infringe on citizens' rights and freedoms and personal privacy.

Along with this view, participants felt that the government should be focusing more effort and resources on the prevention of terrorism and addressing factors that contribute to radicalization and extremism through education, social programs, support for immigrants and at-risk groups, community engagement, and public outreach campaigns as an integral part of their national security strategy. These suggestions

stemmed from participants' opinions that government has three roles in developing a national security framework: to be a funding body, policymaker, and a coordinator of agencies and departments involved in national security activities (Public Safety Canada, 2017).

Bill C-59: An Act respecting national security matters

With consultations complete in 2016, the Liberals embarked on reviewing the controversial provisions in the *ATA* and, taking public and expert feedback into account, began crafting new legislation, resulting in the long-awaited Bill C-59: *An Act respecting national security matters,* which would overhaul many of the provisions critics deemed troubling (Public Safety Canada, 2016; Canadian Civil Liberties Association, 2018a). The purpose of this bill was to resolve citizens concerns that the *ATA* allowed government excessive powers in the name of national security and that did not comply with *Charter* rights and freedoms. The bill includes the introduction of four new Acts, including the *National Security and Intelligence Review Agency Act*, the *Intelligence Commissioner Act*, the *Canadian Security Establishment Act,* the *Avoiding Complicity in Mistreatment by Foreign Entities Act,* along with changes to five other Acts. The bill has been commended for limiting provisions deemed to broadly expand security powers, introducing a new accountability body, and limiting CSIS' investigative techniques[1].

Although this bill has been praised for resolving some of the controversial provisions in the *ATA,* some issues remain The Canadian Civil Liberties Association argues that, although a new oversight body would be implemented, further resources are needed for this body to carry out adequate oversight. Additionally, while the bill enhances oversight of government powers and limits powers in some areas, it also increases powers afforded to some government bodies. For example, the Communications Security Establishment (CSE) would be allowed to use more advanced methods to gather foreign intelligence and to act proactively to stop cyber-attacks. Another key concern for critics is that the bill still does not sufficiently clarify what constitutes "national security" and how government shares information under the *Security of Canada Information Sharing Act* – leaving the process of intelligence sharing largely still in the dark (Hall, 2017; Canadian Civil Liberties Association, 2018b).

[1] On June 19, 2018 Bill C-59 was officially assented into law.

In reviewing the changes introduced in Bill C-59, it is apparent that there are still issues that have not been resolved, some of which will be examined in this research. Recommendations are provided to improve the legislation. Ultimately, while the Liberal's public and expert consultations and Bill C-59 is a step forward in the right direction, they missed an opportunity to conduct a wholescale restructuring of Canada's national security framework. It seems as if the changes introduced in Bill C-59 are mostly a mere re-wording of the most controversial parts of *ATA* rather than a re-evaluation of the necessity of these measures. This is particularly troublesome for those elements that infringe on Canadian's rights and freedoms under the guise of security. The communication between government and public of these modified, yet new, national security measures implemented through Bill C-59 needs to be improved and justification for the more stringent measures needs to be provided.

It is clear the goal of achieving harmony between enhancing national security measures and respecting civil liberties remains a complex task that is unlikely to reach a point of agreement in the near future. It will be essential for the government to continue working towards this goal and to remain clear in its objectives. Hence, this research aims to help policymakers in this important task by providing systematic insight into how Canada's national security approach compares to those of close allies, and how national security perspectives can vary. The previous Conservative government maintained the new provisions merely aligned Canada with the national security strategies employed by close allies. One of the backgrounder documents for the *ATA* states "intelligence services in most of Canada's close democratic allies have had similar mandates and powers for many years" (Public Safety Canada, 2015a). However, substantial evidence demonstrating how specific measures of the *ATA* equate to foreign security policies is lacking. Before accepting government suggestions that the *ATA* merely aligns with security measures already implemented by Canada's allies, it is important to investigate the credibility of this assertion. As such, a review of the policies adopted by the Five Eyes will be conducted.

4.2.2. United States: "America first: Patriotism to nationalism"

Since the tragic events of 9/11 and the resulting upheaval of America's sense of national security, the US government has embarked on a series of securitization and anti-terrorism measures (Hattem, 2015). Consequently, US legislation was vastly

expanded in scope and intensity during the Bush administration. The *USA PATRIOT Act of 2001 (PATRIOT Act)* emerged out of these changes and has remained a profoundly influential, and controversial, piece of legislation (Hattem, 2015). Elements of the *PATRIOT Act* have seemingly permeated into each of the Five Eyes national security laws. Set to expire in 2015, President Obama signed the *USA Freedom Act of 2015* that restored several provisions of the *PATRIOT Act* (Hattem, 2015).

Although the Obama administration maintained that the US was still at war and consequently reinstated some provisions within the *PATRIOT Act,* there were attempts to restrain government powers to achieve a more balanced approach between enhancing national security and preserving constitutional rights, such as placing restrictions and oversight on the NSA's surveillance powers (USA Freedom Act, 2015). The Obama administration shifted away from Bush's language of the "global war on terror" and committed instead to promoting democracy and to the idea that US should be a moral leader in the international platform. Although Obama's National Security Strategy (NSS) named "terrorism" as the main threat to US national security, similar to the Bush NSS, the strategy also contained a variety of new topics viewed as "threats" to US national security, including climate change and infectious disease outbreaks. The document contends that strengthening US national security is the main objective of the administration's approach, but the way to pursue this is to focus on issues outside of enhancing government powers and military force – including developing ways to protect the US from homegrown radicalization. This shift from the Bush approach to that of the Obama administration mirrors the political process currently underway in Canada, whereby the Liberals are attempting to scale back some of the Conservative measures while maintaining strong national security powers deemed necessary by government.

With the election of the Trump Administration in 2016, America has experienced a major upheaval in all areas of public policy to establish an "America first" agenda. At the core of this agenda is the proposition that government must put US interests first, which, contrary to the Obama approach, has resulted in the government denouncing agreements with allied nations such as NAFTA and NATO. The Trump administration's view that it has experienced "unfair burden-sharing with allies" is in direct contrast to how the Obama administration perceived national security could be strengthened by working closely with allies. Where the Obama NSS contended diplomacy with allies and a multilateral approach was necessary to reinforce US security, the Trump administration's

NSS rejects this perspective and instead aims to pull away from working with other nations to achieve national security. Although President Trump does state that he will still maintain good relationships with allies, it seems unlikely given his commitment to "America First".

Additionally, the Trump administration's domestically driven NSS has placed a clear emphasis on enhancing tough security measures in the US. This approach diverges from the Obama administration in that border security, threats from jihadi terrorists, and cyber-attacks are deemed to be the greatest "threats" to US national security. The new administrations NSS does not note threats such as climate change or infectious disease as risks concerning to American security. Instead, the NSS directly states it will focus on "intensified" threats from North Korea, Iran, "radical Islamist terror groups" and "criminal cartels" (United States, 2017). The introduction to the NSS repeats language such as "defend, combat, strengthen, defeat, dismantle" when discussing how to best achieve national security, rather than discussions of diplomacy and multi-faceted approaches. The administration does cite serious concerns over homegrown radicalization, but instead looks to expand government tools to combat this threat, especially enhancing cyber-tools. The enhancement of cyber-tools used by intelligence agencies is expected to reinvigorate debate over the power these provide government agencies and the impact this has on citizens' privacy rights. Contrary to the Obama administration, managing threats of homegrown radicalization will be tackled through new approaches not yet fully provided to the public. Rather than expanding programs aimed to address the root causes of domestic radicalization and extremism, such programs were deemed ineffective and in need of review. Consequently, the Trump administration proposed sharp cuts to domestic terrorism programs and discussed eliminating those deemed ineffective, including programs focused on extremism preparedness and prevention. This move has been intensely criticized by some experts, who perceive this as having a detrimental impact on domestic extremism and as pushing to shift more funds to strengthen the US military force (Kopan, 2017). This is also contrary to the current Canadian national security approach, under which the Liberal government has increased funding to its domestic counter-radicalization programs and created the Office of the Community Outreach and Counter-radicalization Coordinator (Ryerson, Hiebert, & Brooks, 2017).

The Trump administration has yet to propose any significant changes to national security legislation, but this is likely to occur in 2018 following the release of their NSS. Despite the US government's new "America First" approach that treats other nations as competitors rather than allies or adversaries, the Five Eyes arrangement remains intact as it is viewed as benefiting the US. Interestingly, the US has been under criticism by the rest of the Five Eyes. The US experienced a high-profile intelligence leak regarding the Manchester bombing when sensitive information was disclosed in May, 2017. This greatly upset the UK government and shook the foundations of trust among the Five Eyes (Cohen, 2017). Such leaks are highly problematic and violate the intelligence sharing arrangement, where each country is expected to be able to manage and control the information. Without this foundation, the trust that connects these countries becomes jeopardized. That said, the US intelligence regime is an integral part of the Five Eyes and each country greatly relies on intelligence gained through the US intelligence apparatus. As such, the Five Eyes arrangement will remain unchallenged despite criticisms of US government intelligence management. The US remains a source of power in the global realm, and the way it approaches national security and issues of terrorism will continue to affect each of the Five Eyes (Jamshidi & Noori, 2017).

4.2.3. United Kingdom: "Human rights can't stop us"

National security legislation in the UK has been delineated in a series of *Terrorism Acts* beginning in 2000, with the most recent being the *Counter-Terrorism and Security Act 2015.* The UK has become notorious for its volume of national security legislation, as well as the growing severity of these legislative changes (Roach, 2011). The UK government has generally placed a more discernible value on strengthening national security over safeguarding the liberties of its citizens (Moran, 2005). The UK's determination of the most significant threats to the nation have remained fairly consistent since the NSS 2015, focusing on: "state-based threats, terrorism and extremism, and cyber-threats (NSSSDSR, 2015). The UK government appears to have based its security-centric approach on the terrorist incidents it has experienced and employing a preemptive approach. Indeed, current Prime Minister Theresa May's speeches regarding national security make the government's approach quite clear: "...at a time of heightened security threat, it is essential our law enforcement, security and intelligence services have the powers they need to keep people safe" (Burgess, 2017).

Following this policy perspective, in the wake of the 2017 London Bridge and Manchester attacks, the UK government worked towards increasing security measures to a level unprecedented for the UK. When discussing her terrorism strategy, Prime Minister May stated “And if human rights law stop us from doing it, we will change those laws so we can do it” (Mason & Dodd, 2017). As such, the UK government has already introduced and passed the *Investigatory Powers Act* in 2016, which was deemed one of the most extreme surveillance laws passed in a democracy by the *Liberty* human rights group (n.d.-a). This legislation aims to combat the opportunities the Internet provides terrorists to recruit others and spread propaganda, and consequently allows for security services to hack into computers, networks, mobile devices, and servers. This is described as “equipment interference” in the legislation and is available to police and intelligence services, although warrants must be obtained in order to use them. The *IPA* also allows for the bulk collection of data, access to web history data, “bulk personal datasets”, and “bulk hacks” where, if a warrant is granted, security services are allowed to gather data from a large number of devices in a certain location. This bill has been heavily criticized by experts who have labelled it the “Snooper’s Charter” (Liberty, n.d.-a). The human rights group *Liberty* launched an official legal challenge against the legislation due to the level of state surveillance that it permits, which critics deem to be highly intrusive and a clear violation of citizens rights. Despite this pushback, the May administration is working to change national security legislation further by introducing new investigation measures, including curfews and limits to communication devices and increasing the time terror suspects can be held without trial (which is currently 14 days). She has also noted the government may review the UK *Human Rights Act.* Following this path of legislative changes it is clear that the UK’s national security strategy is moving towards increasing prioritization of security measures in favour of protecting democratic rights. This is in contrast to what is happening in Canada and is even more aggressive than the current US strategy, However, contrary to the current US approach, the UK still places value on working with its allies to combat the global threat posed by terrorism and extremism, and intelligence relationships are viewed as an integral part of the UK’s national security strategy and combating terrorism (Vale, 2016).

4.2.4. Australia: “Strong and secure”

Contrary to the political shifts in Canada and the US with regard to national security, Australia has had relatively stable consensus across all parties that robust and tough national security measures are necessary to protect the nation. The Australian government has shared a fairly consistent view on national security since the 2000s, with an emphasis on enhancing strong measures to combat terrorism, cyber-attacks, and espionage. However, unlike Canada, the US, and the UK, 9/11 was not the first major catalyst for the Australian government embarking on a series of changes aimed towards enhancing its national security strategy. Rather, significant legislative changes began in preparation for the 2000 Sydney Olympic Games security operation, as the Australian government was wary that the Olympics could be a prime opportunity for terrorist organizations to gain an international stage. The government focused on enhancing the powers of Australia’s Security Intelligence Organisation (ASIO). Legislation expanded ASIO’s ability to collect data through the use of tracking devices, remote access to computers, and a broad new type of warrant that would allow the agency to intercept telecommunications between a person or foreign organization. Such measures were deemed effective given that these Olympic Games were free of any terrorist incidents.

While Australia’s national security strategy was shifting prior to 9/11, this event served as a significant driver for the government to pass more legislative changes and new offences aimed to strengthen its national security strategy. Prior to 9/11, Australia did not have any specific legislation to address the threat of terrorism; instead, this type of activity was punished under criminal legislation. In the wake of the Bali bombing on October 12, 2002, where 89 Australian lives were claimed, the Australian government discernibly shifted its approach. In order to protect the nation, certain rights and freedoms would have to be curtailed. This approach was demonstrated through various pieces of legislation that specifically targeted terrorist activity and terrorist organizations, and implemented through new measures such as banning certain political groups, allowing for preventative detention and for security agencies to hold semi-secret trials, and imposing conditions on individuals including the requirement to wear a tracking device and restricting their communications with others and through telephone or internet (see Australian National Security Law, 2017 for full list; Rix, 2006). Evident in these pieces of legislation is the fact that the Australian government perceived

homegrown terrorism and foreign fights to be significant threats to the nation's security. The government states the primary threat of homegrown terrorist attacks comes from "Islamist extremists, principally lone actors or small groups".

In 2014, two significant pieces of legislation were introduced and passed in Australia that further reflected the government's position that strong security measures sometimes require civil liberties be limited. The 2014 *National Security Legislation Amendment Bill (No. 1) 2014* introduced national security measures, including allowing security agencies to get a warrant that encompasses an entire computer network and giving ASIO criminal immunity when engaging in "special intelligence operations". The 2014 *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act* introduced new anti-terrorism legislation that provided ASIO further power to share information about terror suspects, allowed for individuals passports to be suspended for 14 days, changed the term "terrorism activity" to the broader term of "terrorism" in legislation, and lowered the threshold for already controversial preventative detention orders.

The national security strategy in Australia appears to be following the same policy trajectory as the US and the UK. This includes increased government powers and new offences to target terrorism as a way to strengthen domestic national security in 2016 and 2017. This includes a law that allows the government to detain individuals without charge for 14 days and can be applied broadly – including children as young as 14. The current party leader, Prime Minister Malcom Turnbull, has voiced his perspective that citizens' rights and national security should be balanced and has defended the proposed laws by stating they are necessary "based on experience" the government has had in successfully disrupting previous terror plots. Yet the Turnbull government's proposed legislative changes to enhance national security have been deemed draconian by some and clear breaches of constitutional rights by critics and civil liberties groups (Karp, 2017; Prime Minister of Australia, 2017).

4.2.5. New Zealand – "All hazards – All risks"

While New Zealand also strengthened its national security approach following 9/11, the country's enactment of national security legislation has not been as far-reaching or numerous as the rest of the Five Eyes. The milder legislative framework implemented in New Zealand may be linked to the country's "low" terrorist threat

designation (Walker, 2014). Contrary to the rest of the Five Eyes, New Zealand government perceives national security to encompass more issues outside of the traditional scope of security stating it takes an "all hazards-all risks" approach to national security. Such unconventional risks include natural hazards, biosecurity, and pandemics. Unlike Canada and the other Five Eye nations, New Zealand's stated strategy doesn't designate domestic terrorism as its main security threat.

The New Zealand government aims to tackle its "all hazards" approach and ensure certain "conditions" that underpin a strong national security framework are maintained through a "holistic" and flexible national security approach and emphasizes the importance of resilience and good governance to do so. This contradicts language used in the rest of the Five Eyes security strategies, which seem to unilaterally emphasize protection and defense as the top ways to achieve national security. Additionally, New Zealand's strategy states it aims to achieve a strong national security regime by keeping measures cost-effective, strategically focused, and accountable to oversight and review. Rather than oversight being tacked on to legislation, as it seems to be in the rest of the Five Eyes security measures, New Zealand's strategy places an explicit importance on oversight throughout the entirety of its national security strategy (Department of the Prime Minister and Cabinet, 2016).

Nevertheless, New Zealand did introduce two main pieces of national security legislation as a response to the events of 9/11; the *Terrorism Suppression Act 2002*[1] and the 2003 Counter-Terrorism Bill. While the *Terrorism Suppression Act 2002* focused on designating terrorists and outlining offences for supporting terrorist organizations, the Counter-Terrorism Bill (2003) broadened terrorist-related offences and expanded police investigative powers. Still, the measures enacted in these pieces of legislation pale in comparison to the expanded provisions introduced in the rest of the Five Eyes. The government's strategy also continuously emphasizes that its approach and agencies be guided by democratic principles – demonstrating their intent to maintain a balanced approach to security and civil liberties. The difference in New Zealand's national security approach is likely influenced by the fact that this nation has a much smaller geographical range and population and is the most isolated of the Five Eyes. Due to their geographical and population differences, however, it is difficult to compare New Zealand with the rest of the Five Eyes. While New Zealand's drive to maintain citizens' rights is a goal to be strived toward, it is important to remain cognizant that New Zealand is a far

smaller country that has been less exposed to issues with domestic national security issues and thus a different degree of perceived threats than the rest of the Five Eyes (Cullen & Reddy, 2016).

4.3. Overview of National Security Measures

4.3.1. Speech-Related Terrorism Offence

Canada

The *ATA* extended speech provisions with the intent of criminalizing speech encouraging terrorist activity. Specifically, section 83.221 introduced a new speech-related criminal offence of promoting or advocating terrorism (*Criminal Code,* 1985). The new speech offence appears to be a pre-emptive measure in deterring the development of terrorist-related activity ("Minister Blaney," 2015). The previous Conservative Minister of Public Safety stated the offence aimed to control and remove online terrorist propaganda used to radicalize and recruit individuals ("Minister Blaney," 2015). Although it is specified that the new speech-related offence will safeguard *Charter* protected rights to freedom of expression, legal experts predict this offence will be challenged in future court cases (Roach & Forcese, 2015b)

For many critics, the introduction of this speech-related offence was by far the most troubling aspect of the *ATA* (Ruby & Hasen, 2015). Legal experts argued that the offence will limit and violate freedom of speech rights protected by the *Charter* (Roach & Forcese, 2015b). It was also suggested that the new offence compromises public safety, as individuals are prevented from engaging in legitimate speech and communicating grievances. For instance, some critics were concerned criticism of government or dissent would be captured under this offence. Additionally, critics argued that extremist views are likely to become more covert and difficult to monitor, and that this will disrupt current counter-radicalization approaches that operate through open dialogue.

Relatedly, the *ATA* implemented the new term of "terrorism offences in general" (*Criminal Code,* 1985, s.83.221). Critics argued this term was deliberately structured to be broad and ambiguous, permitting the offence to apply to a potentially unlimited range of conduct. The offence can also be applied if the individual's statement advocates or promotes terrorism offences while "knowing that any of those offences will be committed

or being reckless as to whether any of those offences may be committed…" (*Criminal Code,* 1985, s.83.221). The use of the word "may" substantially increases the liability on a speaker and significantly lowers the requirement of knowledge in determining culpability (Roach & Forcese, 2015b). Overall, opponents of the offence agreed the addition of this term was unnecessary and unwarranted (Ruby & Hasen, 2015). Roach & Forcese (2015b) explained how the previously existing terrorism-related offences provided sufficient criminalization against speech promoting terrorist activities. Further, offences related to hate speech, counseling an offence, and providing operational instructions about committing terrorist-related activities could also be used to criminalize the promotion of terrorist-related activity [Roach & Forcese, 2015b; *Criminal Code*, 1985, s.319(2), s.22(1), s.83.21(1)].

Skepticism over the advocacy offence was affirmed by the majority of public participants during the Liberals' National Security Consultations. Many individuals emphasized the need to ensure definitions that could impede freedom of expression or speech were clearly outlined. As such, participants took issue with the broad term of "terrorism offences in general" and felt the offence of "promoting or advocating" terrorism could be broadly and subjectively interpreted. In the responses and during consultations, participants and organizations called for the advocacy offence to be clarified so that it is linked to counselling. Participants, however, remained divided on whether they would like to see the part about advocacy or promotion of terrorism offences in general removed from the definition, with 40% in favour and 43% opposed.

Bill C-59 keeps this provision in *SCISA* but attempts to address the above concerns by clarifying that "advocacy, protest, dissent and artistic expression" are only considered unlawful if carried out in conjunction with an activity that undermines Canadian security. This is still problematic, however, and really does not resolve the issues with this part of the offence. These issues will be reviewed in the conclusion and recommendations section.

US

While the US still remains at the forefront of strict national security legislation, the government maintains that freedom of expression will remain safeguarded (Hattem, 2015). Unlike the terrorist-related speech offences found in Canadian, UK, and Australian national security laws, the US has only indirectly restricted speech supporting

terrorism, through the enactment of section 2339A of the *United States Code (USC).* Section 2339A was first enacted by the *PATRIOT Act* and later codified into the *USC.* This section makes "providing material support to terrorists" a criminal offence (*USC,* s.2339A). "Material support" is defined to include "training," "expert advice or assistance," and "service" (*USC,* s.2339A). The US relies on this offence to prosecute speakers who are linked to terrorist organizations and activities (Barak-Erez & Scharia, 2011).

Concerns have been expressed over section 2339A since its introduction in 2001, the contention being that this offence was unconstitutional as it could potentially infringe upon freedom of speech (*USC*). In the 2010 landmark case of *Holder v. Humanitarian Law Project,* the US Supreme Court determined that providing advice to a designated terrorist group about non-violent conflict resolution strategies invoked the offence of providing "material support to terrorists" (*USC,* s.2339A). This ruling determined the constitutionality of s. 2339A in US law and solidified the offence as a legitimate preventative measure against terrorist-related activity. The judges acknowledged this limited freedom of expression to a certain degree, but did not entirely compromise freedom of speech (Cole, 2012). The decision in the *Holder v. Humanitarian Law Project* (2010) has been criticized for limiting the scope of political freedom and jeopardizing First Amendment freedoms related to speech. Those opposed to the decision argue that it has "dramatically expanded government authority to suppress political expression and association in the name of national security" (Cole, 2012, p. 149).

Despite these comments, the US at least applies certain criteria to when speech can be connected to terrorist activity. This is the type of criteria clarification that could strengthen Canada's speech-related terrorism offence as it provides clear guidelines on how this offence will be interpreted and applied in court. By leaving legislation unclear on how it can be applied, cases involving these offences, and especially those that infringe on Charter rights, could be taken to the Supreme Court for judicial interpretation. This can result in an offence being struck down – making this national security-related offence ultimately ineffective to meeting its stated objectives. Having criteria outlining how an offence will be applied strengthens the legislation by providing clarity of its potential application.

UK

The UK terrorism offences relating to expression and speech were implemented almost a decade prior to the ATA. The *Terrorism Act 2006* was introduced as a response to the 2005 London Bombings ("Terrorism act 2006," 2009). Within the *Terrorism Act 2006*, Section 1 criminalizes direct and indirect "encouragement of terrorism." While nearly identical, the structure of this offence slightly diverges from the Canadian equivalent. Rather than applying to "terrorism offences in general," the UK offence applies in situations where an individual's statement encourages another in the "commission, preparation or instigation of acts of terrorism or Convention offences" (*Terrorism Act,* 2006*,* s.1) The provision outlines the offence can be applied if the person or group either "directly" or "indirectly" encourages or induces others to engage in terrorist-related activity (*Terrorism Act,* 2006)

Criticisms of the speech provisions in the UK parallel those in Canada, where legal scholars and civil liberties organizations argue the speech offence is over broad and violates freedom of speech rights (Liberty, n.d.-b). Critics maintain this offence produces a chilling effect on free speech (Liberty, n.d.-b). It is argued these provisions stifle the ability for citizens to speak out freely against certain political or repressive regimes, domestic and international political issues, and foreign policies (Liberty, n.d.-b). The United Nations Human Rights committee has even criticized the UK provisions for interfering with human rights and violating freedom of expression ("Terrorism Act 2006," 2009).

Australia

In 2014, the Australian government enacted the *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act*. This omnibus legislation implemented a series of amendments to improve the legislative national security framework and better respond to the evolving security threats posed by foreign fighters (Attorney General, 2014). The amendments to the *Criminal Code Act 1995* included the creation of an "advocating terrorism" offence (s.80.2c). Similar to the Canadian provision, the offence applies whether the individual advocates terrorism knowingly or recklessly. Unlike the current Canadian counterpart, the Australian legislation provides a definition for advocating terrorism. Advocating refers to any "person [who] counsels, promotes, encourages or urges the doing of a terrorist act or the commission of a terrorism offence" [*Criminal*

Code Act 1995, s.80.2(c)(3)]. The Australian offence also defines and outlines a "terrorist act" and "terrorism offence," in contrast to the *ATA's* broad reference to "terrorism offences in general." Furthermore, the Australian provision specifies the offence will not be invoked if incitement relates to an attempt or a conspiracy to attempt a terrorist offence [*Criminal Code Act 1995,* s.80.2c (2)(i)(ii)].

Although the Australian legislation does define some of the language used in the provision and employs a more restricted application of the offence, the language used is still considered problematic. Legal experts argue the words "encourage" or "urge" may be open to interpretation in court (Roach & Forcese, 2015b). As well, this speech-related offence raises identical concerns to those expressed in Canada, the UK, and the US. Critics suggest this offence has a chilling effect on free speech and expression (PIAC, 2015). The Public Interest Advocacy Centre ([PIAC], 2015) anticipates the offence will have a "normalising effect of gradually limiting speech over successive pieces of legislation" (p. 9). Consequently, the PIAC (2015) has urged the Australian government to repeal the advocating terrorism offence.

New Zealand

Contrary to Canada and the other Five Eyes members, New Zealand's national security legislation does not contain a specific provision criminalizing the incitement of terrorist-related activities. New Zealand instead relies on other provision within their criminal law to criminalize incitement of terrorism. New Zealand has legislation prohibiting the "incitement, counseling, or attempt to procure any person to commit any offence," even if "that offence is not in fact committed" (*Crimes Act 1961,* s.311(2),). Section 81 of the *Crimes Act 1961* outlines seditious intention offences, where it is an offence "to incite, procure, or encourage violence, lawlessness or disorder." Other offences in New Zealand's criminal law, such as making threats of harm and party offences, could also be potentially used to prosecute advocacy or incitement of terrorism. However, the above offences only apply to domestic situations and have a variety of limitations.[2] [2] Thus, New Zealand laws are practically incapable of prosecuting an individual who has incited others to commit terrorist-related activity abroad (Conte, 2010).

[2] See Conte (2010) for a detailed analysis of New Zealand's laws and the associated limitations.

New Zealand's national security regime has been praised for maintaining a fairly proportionate balance between strengthening national security and protecting civil liberties (Smith, 2003). The New Zealand *Bill of Rights Act 1990* protects the rights of citizens to engage in "freedom of expression, including the freedom to seek, receive, and impart information and opinions of any kind in any form" (s.14). Yet, criticisms similar to those expressed in the Five Eyes nations suggest New Zealand's national security legislation utilizes ambiguous language susceptible to misinterpretation (Smith, 2003; Human Rights Commission, 2014).

Conclusions and Recommendations

Prior to the enactment of the *ATA*, Canada's restrictions on freedom of speech and expression were not codified directly under national security legislation. With the passing of the *ATA*, Canadian legislation has expanded restrictions on speech encouraging terrorism. While this new speech-related offence is argued to be overly restrictive, the Canadian government is not the first of the Five Eyes community to invoke this type of offence. In fact, the UK implemented a speech-related terrorist offence nearly a decade prior to the *ATA*. Nonetheless, Canada's restrictions on speech now compare to strict UK and Australian provisions. The structure of Canada's "advocating" or "promoting" terrorism offence borrows language directly from the equivalent Australian offence (Department of Justice, 2015). However, the Canadian application of this offence to "terrorism offences in general" invokes a much broader scope than the Australian counterpart (*Criminal Code,* 1985, s.83.221).

The new speech-related offence also adopts Australia's low threshold for prosecution. Both countries laws outline the advocacy of terrorism can occur either knowingly or recklessly. The UK also employs similar thresholds, where encouragement can be connected as having either a direct or indirect role in inciting terrorist-related activity. As well, the UK offence contains the most severe punishment for the speech-related offence, where those found guilty could face seven years' imprisonment. The Canadian and Australian provisions outline a maximum of five years' imprisonment.

The US and New Zealand have employed slightly different legislative approaches in managing incitement of terrorist-related activity. The *USC* criminalizes "support" to terrorists in the form of "advice or assistance," but has not crafted an explicit speech-related terrorism offence. While usually demonstrating the toughest approaches to

national security, US legislators are extremely hesitant to introduce or support legislation that could potentially impede First Amendment rights to freedom of speech, even despite increasing concerns over extremist-supporting speech on the Internet and social media (Haugham, 2016). Unlike the other Five Eyes members, New Zealand still relies on existing laws outlined in different legislations to prosecute incitement of terrorism and does not have any specific provisions within national security legislation directly criminalizing incitement of terrorism. Despite slight departures between the Five Eyes, national security legislation across the members appears to have developed provisions that comply with the United Nations Security Council (UNSC) Resolution 1624 of 2005. Developed in response to the London Bombings in 2005, Resolution 1624 called upon all states to condemn "incitement of terrorist acts and repudiating attempts at the justification or glorification of terrorist acts that may incite further terrorist acts…" (p. 1).

The concerns expressed over the speech-related terrorism offences in each of the Five Eyes are nearly identical. It is argued the legislative changes permit governments to suppress free speech and political expression. Critics predict the speech-related offences will have a significant chilling effect on speech. This can have negative repercussions, such as intensifying grievances and subsequently fostering extremism. While the specific details vary, the speech-related offences adopted by the Five Eyes community, excluding New Zealand, are believed to undermine democracy and compromise national security (Capoccia, 2013).

Originating from a concern over online radicalization and recruitment, the new speech offence is an attempt to deter those who promote terrorism through criminalization (Public Safety, 2015). While it is agreed that the threat of radicalization and recruitment is growing and measures are needed to manage this threat, the new speech offence could have serious impacts. The potential of driving extreme dialogue discussions offline and having them take place in further secrecy are echoed amongst critics in all Five Eyes. Many of these critics agree the online realm provides an opportunity for monitoring and investigating extreme dialogue and processes of radicalization (CBA, 2015).

Although critics of this provision have urged the Liberal government to remove the new speech-related offence to protect freedom of speech and expression, the introduction of this offence is not out of line with national security legislation among the

Five Eyes. The changes introduced in Bill C-59 do make an attempt at clarifying when this offence can be applied to speech, however, critics assert the language used in section 83.221 will still be susceptible to subjective interpretation. Moreover, Forcese & Roach (2015c) demonstrate extensively how existing offences can already be applied to speech inciting terrorist activities and how these provisions could be reformed and strengthened without the need for the advocacy and promotion offence.[3]

Given the concerns outlined above, and the fact that the Canadian public remains divided on whether an offence related to the term of "promoting" a terrorist offence should be legislated, it is recommended that government amend the offence to include more specific details about how this offence could be applied and the elements required. This would require the government to enact criteria to ensure the offence is capturing only the behavior it intends to criminalize. For example, the US makes a distinction on its speech-related terrorism offence by requiring speech to be linked to advice or assistance, which necessitates a more direct linkage between an individual's statement and a tangible action. Criteria such as this needs to be implemented by Canada to clarify the ambiguous language and constrain future governments from excessively applying the offence.

Additionally, Canada's current language is problematic because it is clearly adopted from Australia's provisions, which remain highly controversial given the ambiguous language and unclear application. These critiques should have been taken into consideration when crafting this offence as a way to engender confidence among the public that this offence legitimately restrains freedom of speech and expression. The need for clarity is based on distinguishing between offensive and dangerous statements. On the one hand, an individual's statement applauding terrorist incidents may be offensive to the majority of individuals and society. This is very different, however, from statements that have clear intent of inciting others to plan or commit dangerous action that could harm others. As such, it is recommended that the legislation be amended so that, in order for it to be criminalized, comments or expression require clear intent with a reasonable expectation that the crime will be carried out. This criteria would align with the goals of the offence - to criminalize dangerous activity and not offensive activity. This

[3] See Forcese & Roach (2015c) for an in-depth discussion of section 83.221 of SCISA and the alternative proposal they offer.

additional criterion would not unduly restrict the offence, either. Indeed, it could still be used as a preemptive offence given that it would apply to an individual who made a direct call to violence where there is substantial risk another person could act on such comments. This would present a sufficient relationship between the problematic speech and the potential act.

Although Bill C-59 adds in that "advocacy, protest, dissent and artistic expression" are only considered unlawful if carried out in conjunction with an activity that undermines Canadian security, this still leaves room for non-dangerous actors to be wrongfully prosecuted. While this section is intended to demonstrate that government will protect against the application of this offence to those particular cases, the problem remains that government only need to argue such cases as being an activity that undermines Canadian security. As such, this particular re-wording does not truly protect against government applying this offence in these cases. As an example, activists opposed to the Trans Mountain pipeline in BC, now owned by the federal Canadian government, may promote or encourage others to disrupt construction through comments at a rally or online. Such comments, under the current legislation, could be deemed as inciting acts that undermine Canada's security. This is because the pipeline could be considered critical infrastructure – of which both the *ATA* and Bill C-59 intend to protect as an essential part of Canadian domestic security. As such, the legislation is over broad and should be constrained. If a comment or statement can be clearly demonstrated as having intent to cause harm and meet criteria such as aiding, assisting, or specifying what action an individual should take, knowing that the individual is likely to commit such an act, then there is a justifiable reason to criminalize this conduct. However, absent such criteria, comments made at a protest or in dissent with government should not leave an individual open to being charged with a terrorism offence.[4]

More extreme examples of how this offence could be improperly applied without clear criteria can be seen in Spain. Spain's government has a similar terrorist-related offence of 'glorifying' and 'encouraging' terrorism. In 2018, a rapper was jailed for three years for using aggressive lyrics such as "we want death for these pigs" in reference to

[4] Bill C-59, passed on June 19, 2018, implemented the requirement where a person specifically "counsels another person to commit a terrorism offence." This provides a clearer structure around the offence and how it can be applied, which meets the provided recommendation.

politicians and members of the monarchy (Loughrey, 2018), Again, while such comments can be considered offensive and aggressive, it is argued this does not fall under the umbrella of “terrorism” until it can be proven these lyrics present a real threat whereby the individual has the intent to cause real harm or such statements could aid others in carrying out such action. Another case in Spain involved a student making a joke on Twitter about the 1973 assassination of Luis Carrer Blanco, a right-wing prime minister who was killed in a bombing by the Basque separatist group ETA. The student received a one year prison sentence, although this was eventually overturned in the Supreme Court (Jones, 2018). The new speech-related legislation in Canada raises questions about whether comments made about past terrorist incidents in Canada, such as the Air India bombing or the death of Pierre Laporte by the Front de liberation du Quebec (FLQ), could be interpreted as “promoting” or “advocating” terrorist activity. Again, while such comments in the form of a song or joke are considered morally offensive and inherently violent, it is argued the potential application of this offence to those situations would be excessive and unjust. Offensive remarks, disdain for authorities, or criticism of perceived injustice do not constitute legitimate restrictions of freedom of speech.

While Canada is not alone in implementing a “promoting” and “advocacy” speech-related terrorist offence among the Five Eyes, the term is controversial in each nation. The crux of the issue is the ambiguity around what type of speech would induce the offence and such an offence could be aggressively enforced, despite current government claims that they would not tackle lawful activism or artistic expression. Any offence that limits a citizen’s democratic right needs to be clearly defined and understood by the public. This requires further consultation between government and the public, with the need for government to reassess the limits to this offence and to outline the legitimate risks this offence aims to tackle with clear application.

4.3.2. Increased Information Sharing Practices: Security of Canada Information Sharing Act

Canada

One of the most controversial components of the *ATA* was the enactment of the *Security of Canada Information Sharing Act (SCISA*). Under Part 1 of the *ATA*, this act permits information sharing between government institutions in order to combat "activity that undermines the security of Canada" (*SCISA,* 2015, s.2). Section 2 outlines examples of these activities, including terrorism and critical infrastructure interference. However, section 2 can be extended to include any activity that "undermines the sovereignty, security or territorial integrity of Canada…" (*SCISA*, 2015). Under these circumstances, the government is authorized to share information for investigative purposes. Some of this information is "big data," which uses massive amounts of citizen information in order to identify trends and predict the behaviour of individuals or groups (Roach & Forcese, 2015a). While government institutions already share information with each other for national security purposes, *SCISA* will further relax legal barriers preventing or delaying the exchange of information.

Government institutions have authority to share information proactively or upon request under *SCISA* [s. 5(1)]. The government has provided this authority to 17 institutions deemed to have "national security responsibilities" (*ATA*, 2015). These government institutions range from security services, such as CSIS and RCMP, to health, border control, finance, and transport agencies. Section 5 also states the heads of these government institutions or their delegates can have access to shared information, while section 6 allows disclosure of information to "any person, for any purpose" if "in accordance with the law" (*SCISA,* 2015). The act indicates only these institutions and individuals are permitted to share information when relevant for national security purposes. Moreover, information sharing practices will remain accountable to provisions of the *Privacy Act 1983* and operations subject to review by the Office of the Privacy Commissioner to ensure the privacy of Canadian citizens is respected (Public Safety, 2015).

The purpose of *SCISA* (2015) aims "to encourage and facilitate the sharing of information" among government agencies in order to better protect Canada and its citizens (s.3). Public Safety (2015) maintains the government's ability to share and

access information through an “accurate, timely, and reliable” process is essential when faced with threats to national security (“Information Sharing and Canada’s National Security”). Information sharing between government agencies is deemed to be necessary in managing the “diverse and complex threats” posed by terrorist groups (“Information Sharing and Canada’s National Security”). On these grounds, the Conservative government maintained most Canadians will support information sharing to preserve public safety and national security (James, 2015).

However, there was immense opposition to the information sharing changes implemented through *SCISA*. Many critics argue the government has not made a convincing case as to why information sharing should go unconstrained between departments. Instead, it is suggested *SCISA* will have disastrous privacy consequences. Roach and Forcese (2015a) outline the privacy implications of *SCISA* due to the ambiguous language used in the bill, the broad scope of information sharing, and the deficient privacy safeguards. The Maher Arar case is highlighted to demonstrate past injustices stemming from unreliable information sharing (Roach & Forcese, 2015a).

Recognized among critics of *SCISA* is the unprecedented scale of information sharing between government agencies. *SCISA* allows government agencies to access and share vast amounts of citizens personal information (Roach & Forcese, 2015a). This can facilitate the misuse of personal information and the violation of privacy rights guaranteed to Canadians. Roach and Forcese (2015a) argue the broad language used in Section 2, outlining activities that “threaten the security of Canada,” allows for the authorization of information sharing under any circumstances (*SCISA,* 2015). Although Section 2 excludes “lawful advocacy, protest, dissent and artistic expression” from being considered threatening activity, Roach and Forcese (2015a) argue that these activities can easily be deemed unlawful due to non-compliance with regulatory rules (*SCISA,* 2015). Consequently, activities such as labour strikes, environmental activism, and Aboriginal protest may trigger the information-sharing regime. The CBA (2015) argues these activities should not be equated to national security threats, as they are important elements of a “free and democratic society” (p. 12). As such, the bill is criticized for being applicable to a range of activities that do not pose a threat to national security.

Another major criticism of *SCISA* is the lack of effective oversight. Roach and Forcese (2015a) argue *SCISA* lacks sufficient accountability measures and safeguards to ensure information being shared is reliable, relevant, and securely controlled by the agencies. The Auditor General and the Privacy Commissioner are currently charged with the responsibility to review information sharing practices (Public Safety, 2015). However, Roach and Forcese (2015a) identify a major gap in this arrangement; neither the Auditor General nor the Privacy Commissioner are mandated to ensure information sharing is being conducted in accordance with the law. Moreover, the Privacy Commissioner has been urging for reform of the *Privacy Act* for many years now due to deficiencies in accountability and oversight (Roach & Forcese, 2015a). These concerns were also recognized in the 2006 Arar Commission report. The report outlined how the oversight agents of government information sharing are considerably limited by jurisdictional restrictions (Arar Commission Report, 2006).

Additionally, a judicial redress mechanism is absent for individuals who believe they have been wrongly watchlisted as national security threats (Roach & Forcese, 2015a). Due to the covert nature of government information sharing, individuals may not even be notified their personal information has been shared and investigated by government institutions. Roach and Forcese (2015a) have likened the misuse of information to a “privacy virus...that will be very difficult to remedy” (p. 10). Once information has been shared between the different government agencies, it will be an arduous process for individuals to have their information cleared and secured again.

Due to the outlined concerns over *SCISA*, this *Act* and its provisions remain highly criticized. Critics of *SCISA* believe massive information sharing between governments is excessive, disregards Canadians privacy rights, and lacks adequate oversight to ensure this information is reliable and not falling into the wrong hands (BCCLA, 2015; CBA, 2015). This concern was evidently shared by the majority of the public during the National Security Consultations, where the majority felt strongly that government needs to clarify the process outlined in *SCISA*. Similar to the speech-related offence, participants felt definitions within this *Act* were too vague and could be extended to a variety of activities under the current wording that could infringe personal privacy. Participants called for increased oversight of government operations under *SCISA* and for further regulations to keep agencies accountable – such as keeping a record of disclosure when information-sharing occurred.

A positive change brought forth to address these concerns in Bill C-59 is changing the concept of information sharing to information disclosure. The purpose of this is to clarify that no new information is being collected under this *Act* but rather information is being disclosed for investigations. As well, the bill attempts to emphasize that personal information will only be shared in situations where it is necessary for national security. Specific changes include the further expansion of the definition to "activity that undermines the security of Canada" to add clarification. These changes include the extension that the "activity" could threaten the lives of people who live in Canada or those who have a connection to Canada but lives outside the country. Preceding the examples of what could constitute activities that undermine the security of Canada, such as interference with critical infrastructure and global information infrastructure, the bill adds the words "significant or widespread".

Additionally, the Liberals did introduce and successfully pass a bill in 2016 that created a parliamentary oversight committee to review national security operations. Bill C-22: *An Act to establish the National Security Intelligence Committee of Parliamentarians*. This *Act* outlined that the oversight committee would be composed of bi-partisan MP's and Senators and would thus be able to oversee multiple government agencies and review their security operations. This was a major step forward in addressing concerns that Canada's national security procedures were missing an overarching body that was specifically mandated to review national security operations among a variety of agencies, including CSIS, the RCMP, CSE, and the CBSA. Two problematic components of this committee are a) its members are appointed by the Prime Minister rather than Parliament; and b) the committee's recommendations are not binding. This is seen to be an issue as it could undermine the impartiality of the group that is in charge of likely reviewing security decisions involving the Federal government, as well as their ability to have any real power when it is determined that government has overreached their boundaries in the name of national security. Critics of the committee's current structure also identify problems such as the government's ability to block investigations on the ground of ongoing national security operations and limiting access to certain documents and information – restricting the committee's ability to properly fulfill their mandate (International Civil Liberties Monitoring Group, n.d.).

It is clear from the feedback of the public, Canadians are extremely sensitive about their privacy rights and the power of government to collect and share information.

This piece of the *ATA* will likely continue to be highly debated and refined to find a balance that satisfies both the public and government; individuals in Canada, and globally, are increasingly becoming privacy-aware in the era of big data, and conscious of unresolved procedures about how government and the private sector are handling and securing personal information. That said, it is recognized that an information-sharing regime is necessary for government agencies to effectively conduct operations and investigations for national security purposes. Such practices, however, need to be conducted when required and under a regulated process that protects the privacy of citizens. Citizens feeling wary about how their personal information is being handled can lead to harmful repercussions in their perceptions and confidence of governance.

US

Similar to Canada, justifications for increased information sharing by US government refer to the rising threat of lone actors and evolving terrorist activities, such as cyber-terrorism. The 2015 National Security Strategy states improved information sharing is critical in combating the threats and hazards of terrorism. In the aftermath of 9/11, the US government embarked on a series of organizational changes to its security and intelligence framework (Tembo, 2014). This undertaking was initiated in response to the 9/11 Commission's suggestion that reform of how government agencies interact and share information with one another was necessary (Vicinanzo, 2015). Consequently, the *USA PATRIOT Act of 2001* (*PATRIOT Act*) removed structural barriers between intelligence and law enforcement to better facilitate cooperation and build a mutual support system in combating terrorism (Department of Justice, n.d.). One of these provisions amended the *Foreign Intelligence Surveillance Act of 1978* to allow FBI officials the ability to exchange information for investigations (Sales, 2010). The *PATRIOT Act* has since expired, but Section 18 of the *USC* authorizes disclosure of wire, oral, and electronic communications between investigative and law enforcement agencies. The *Intelligence Reform and Terrorism Prevention Act of 2004* was also designed with provisions to foster federal government information sharing. Additionally, the *Homeland Security Act of 2002* authorizes disclosure between its component agencies to analyze and share information with state, local, and private sectors partners to monitor suspected threats (Rosenbach & Peritz, 2009).

US security and intelligence legislation continues to allow fairly free-flowing information sharing between government agencies in its counterterrorism efforts. Recently, the White House passed a controversial cyber-security bill authorizing data sharing between the US government and corporations to prevent cyber-attacks on US networks (Risen, 2015a). This was deemed a critical national security measure to better enhance US cyber-security and protect critical infrastructure. A wide range of critics including civil society groups, legal experts, and academics argue the cyber-security bill purposefully contains exceptionally broad language. The structure of these provisions allows law enforcement to investigate individuals "outside the scope of cybersecurity" (Greene, 2015, "Coalition Letter"). Opponents of the new bill suggest this will enable risky information sharing with the NSA and authorizes uncontrolled cyber-surveillance (Risen, 2015b).

Over a decade after 9/11 and the Snowden revelations in 2013, the US continues to experience strong opposition to its information-sharing regime (Tembo, 2014). This opposition parallels the criticisms of Canada's new information sharing structure. The nearly unfettered information sharing within US government agencies raises extensive concern among the public (Guliani, 2015). Despite legislation and policy outlining information sharing procedures, there still appears to be co-ordination issues among the different intelligence and security agencies (Nelson, 2011). In 2013, the Brennan Center for Justice released a comprehensive report examining information-sharing practices among US law enforcement agencies. The report concluded the system was "organized chaos…a loosely coordinated system for sharing information that is collected…with insufficient quality control, accountability, or oversight" (Price, 2013, p. 3). Critics of the US information sharing regime emphasize the need for responsible data distribution accompanied by safeguards to ensure citizens' rights are not abused (Nelson, 2011).

UK

The UK government has also favoured a highly-integrated information sharing system between its security and intelligence community. In the wake of 9/11, the UK began restructuring its counterterrorism strategy to improve its intelligence regime. This reformation aimed to prevent terrorist activities by intervening earlier in the process of recruitment and planning (Field, 2009). A review found cross-agency hurdles existed in information sharing due to a lack of communication between agencies. In response, the

Joint Terrorism Analysis Centre (JTAC) was created in 2003 to increase effective sharing procedures (Gregory, 2005). JTAC operates as an integrated multi-agency team that shares relevant information between the UK police and government agencies in order to "assess the nature and extent" of national security threats (Security Service, 2015, "Role"). Government agencies involved with JTAC range from Security Service agencies, specialized police branches, customs and immigration departments, and special agencies such as the Office for Civil Nuclear Security (Gregory, 2005). JTAC functions as a centralized system, analyzing terrorism-related intelligence and directing this information between these agencies (Gregory, 2005).

Additionally, the Security Service (MI5) collects and analyzes information to provide to the Joint Intelligence Committee (JIC). The JIC is responsible for prioritizing information and providing threat assessments to senior government officials (Security Service, 2015). The *Counter-Terrorism Act 2008* authorized the different circumstances in which the MI5, Secret Intelligence Service (MI6), and Government Communications Headquarters (GCHQ) can disclose and share information. This provision authorizes information disclosure when necessary for these agencies to conduct their functions. These functions include preventing or detecting crime, protecting national security, or when it is necessary to disclose information for criminal proceedings (*Counter-Terrorism Act*, 2008, s.19).

While the UK has been commended for the integrated structure of its intelligence-sharing regime, the system still faces information sharing issues (Field, 2009). MI5 has been criticized for ineffective intelligence sharing, such as failing to pass along information about the shoe bomber, Richard Reid in 2001 (Field, 2009). The GCHQ was exposed for its collection of bulk data in 2013 by the Snowden revelations. A subsequent inquiry found the agency had been collecting data "on an unprecedented scale" (Parliamentary Office of Science and Technology, 2014, p. 4). The intelligence agencies have also been criticized for their unwillingness to share information with local police (Tembo, 2014). Field (2009) notes the agencies are unwilling to share intelligence in fear sensitive information will be exposed. There have also been problems with coordination, such as slow responses to information requests between agencies. The intelligence operations of these agencies are not always aligned, such as domestic and foreign operations, and this can cause agencies to be hesitant in sharing information (Field, 2009).

The Intelligence and Security Committee (ISC), a parliamentary committee consisting of members from various political parties, provide oversight of MI5 and report their evaluation to the Prime Minister (Security Service, 2015). However, review of MI5 is done retrospectively. Critics have suggested this retrospective process allows MI5 to get away with risky activities, such as sharing private information about UK citizens, that are later determined to have violated civil rights (Tembo, 2014). Moreover, the UK government has faced significant legal inquiries into its information collecting and sharing operations. Civil rights organizations argue UK legislation related to information sharing, privacy, and surveillance contains significant loopholes that allow government agencies to infringe on fundamental civil rights (Equality and Human Rights Foundation, 2012). With regard to the Snowden revelations, the ISC ultimately determined GCHQ was lawful in collecting mass data. However, the ISC emphasized the need for more oversight of these activities (MacAskill, Watt, & Mason, 2015).

Australia

The Australian government has also emphasized the necessity of information sharing in achieving an effective national security strategy (Council of Australian Governments, 2015). This type of information coordination and distribution is encouraged through the functions of the Australian Crime Commission (ACC), Counter-Terrorism Control Centre (CTCC), and the National Threat Assessment Centre (NTAC). In a review of Australia's national security framework, the Department of the Prime Minister and Cabinet ([DPMC], 2015) explains how national security legislation relating to information practices has noticeably changed in Australia, stating: "information sharing 'need to know' was replaced with a new motto 'need to share' " (p. 3). Established in 2003, the ACC is responsible for amalgamating information from various national security and intelligence departments. After reviewing information, the ACC provides the Australian government with criminal intelligence assessments to determine security priorities (DPMC, 2015). Departments that share information with ACC include provincial and federal police, customs and tax departments, and the Australian Security Intelligence Organization (ASIO) (O'Connor, 2006). The CTCC is led directly by the ASIO, which coordinates with the Australian Federal Police, the Australian Secret Intelligence Service and the Defence Signals Directorate (O'Connor, 2006). The collection and integration of information obtained from these agencies is used by the CTCC to advise the Australian government on potential threats. The centralized system

of NTAC is also responsible for collecting and analyzing intelligence related to potential threats through coordinating with various government agencies (DPMC, 2015).

Additionally, the ASIO has a mandate to analyze intelligence information and provide terrorist threat assessments to government. This involves collecting information from multiple government agencies (Australia, 2014). ASIO collaborates with "authorities of the Commonwealth, Departments, police forces and authorities of the State and authorities of other countries approved by the Minister" (Australia, 2014, para. 101). With the passing of the National Security Legislation Amendment Bill (No.1) 2014, ASIO is also authorized to coordinate with organizations outside of the government. The bill amended section 19(1) of the *ASIO Act 1979*, to enable ASIO to liaise with any domestic or foreign individuals or groups to perform its activities. This new provision codifies ASIO's ability to cooperate with the private sector. The Australian government justifies this cooperation by maintaining that it is necessary given that Australia's critical infrastructure is dominantly owned by private entities (Australia, 2014). As such, they argue that critical infrastructure is exceptionally vulnerable to security threats, such as cyber-terrorism, and safeguards need to be strengthened. Under the new provision, co-operation between ASIO and the private sector "may involve the sharing of personal information" (Australia, 2014, para. 104). In order to limit the sharing of personal information, the provision requires the Director General to ensure personal information is only collected or disclosed if it "is reasonably necessary for the performance of its statutory functions or other authorized or required by law" (Australia, 2014, para. 105). In regard to privacy rights, the Memorandum for the bill explains potential infringements on citizens privacy is for a "legitimate objective" and may be necessary for ASIO to perform its national security functions (Australia, 2014, para. 107).

Australia has been commended for having a more robust oversight system than the US or the UK. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) and the Inspector General of Intelligence and Security (IGIS) provide oversight of intelligence activities (Flood, 2004). Although the Governor-General appoints the IGIS, this oversight agent operates as an independent body. The IGIS is responsible for holding the intelligence community accountable by reviewing their activities to ensure they conform to the law and respect civil rights (Flood, 2004). Compared to oversight bodies among the Five Eyes, the oversight abilities of the IGIS are considered fairly

robust. Unlike other oversight bodies, the IGIS is authorized “complete access to agency records and strong powers to require evidence” (Flood, 2004, p. 56).

Despite strong oversight, ASIO has been criticized for ineffective and intrusive information sharing (Burch, 2007). Human rights organizations are most notably concerned with the expansion of information sharing between government agencies. In a submission to the PJCIS, the Australian Human Rights Commission ([AHRC], 2014) states the new ability of ASIO to “co-operate” with private entities is far too ambiguous. It is argued this ability provides ASIO an unreasonably wide scope in accessing and sharing citizens’ personal information (AHRC, 2014). Extending this cooperation beyond government agencies to private entities is considered highly problematic. The AHRC (2014) argues private entities cannot be held accountable for information sharing errors like government agencies can be. Thus, the AHRC (2014) has urged the government to delete this provision from the bill as it violates privacy rights and allows for the potential misuse or exposure of sensitive information (Farr, 2016; Fisher, 2016).

New Zealand

The New Zealand Security Intelligence Service (SIS) coordinates with the Government Communications Security Bureau (GCSB) and the National Assessments Bureau (NAB) to form the core of the New Zealand Intelligence Community (NZIC). Information sharing occurs between these three agencies as well as New Zealand’s police and specific government departments, such as customs and immigration (NZIC, 2015a). The SIS is primarily responsible for investigating terrorist activity and security threats. Similar to the other Five Eyes intelligence agencies, SIS is only authorized to share information if such measures are “necessary and proportionate” to protect national security (*NZIS Act*, 1969, s.4(1)]. As well, the SIS is authorized to liaise with foreign security and intelligence agencies in order to exchange information related to security issues, as long as SIS is acting within the law and respecting citizens’ rights (*NZIS Act,* 1969). The Director of SIS has legislative authority to determine whether information will be shared between agencies [*NZIS Act*, 1969, s.1(a)]. The *NZSIS Act* 1969 also outlines that SIS may “co-operate as far as practicable and necessary” with State services and public authorities both within and outside of New Zealand to assist “the Security Intelligence Service in the performance of its functions” [*NZIS Act*, 1969, s.1 (c)]. Moreover, changes were made to the *Privacy Act 1993* in 2013 to allow specific public

services the ability to disclose citizens' personal information if a serious public safety threat is present (Ministry of Justice, 2013).

The New Zealand intelligence oversight regime incorporates a few agencies. The Minister for National Security and Intelligence leads the majority of oversight over security and intelligence operations in New Zealand (NZIC, 2015a). Parliamentary oversight is also provided by the Intelligence and Security Committee (ISC). However, the primary purpose of the ISC is to review NZIC policy and administration (NZIC, (2015a). The Foreign Intelligence Requirements Committee specifically reviews SIS foreign intelligence activities, a specific feature missing in the Canadian oversight regime. The Inspector-General of Intelligence and Security (IGIS), similar to the Australian equivalent, provides independent oversight and investigations (NZIC, 2015b). The IGIS is responsible for ensuring SIS is operating lawfully and respecting civil rights (NZIC, 2015b). However, critics have called into question the ability of both the ISC and IGIS to conduct effective oversight and review (Weller, 2001; Liddicoat, 2014). It is argued these oversight bodies do not provide the public or parliament with sufficient information regarding NZIC activities (Weller, 2001). Critics suggest legislative changes have allowed NZIC agencies to engage in activities that violate rights of New Zealand citizens, such as misusing and disclosing sensitive personal information (Liddicoat, 2014).

Furthermore, in a submission to the New Zealand government, the Auckland Council for Civil Liberties (ACCL) and the Human Rights Foundation of Aotearoa New Zealand (HRF) argue the Minister, the Police, and other government agencies have unnecessary and far-reaching authority in using classified and sensitive information ("Human Rights Submission," 2004). Both groups suggest the need for more effective oversight of how SIS and other government agencies are utilizing citizens personal information. It is argued that the justification to use classified information for "national security" purposes is too ambiguous and potentially unwarranted. The groups advocate for an extensive review and reform of all security legislation in New Zealand ("Human Rights Submission," 2004).

Conclusions and Recommendations

Since 9/11, it is apparent that internal security issues have become a major focus in national security strategies across the Five Eyes community. The implementation of

tough national security legislation has substantially increased the powers of intelligence agencies and law enforcement. All of the Five Eyes governments have emphasized the importance of timely and secure information sharing in strengthening national security approaches. With the *ATA*, Canada appears to be contending with the US, the UK, and Australia in regard to liberal information sharing between government agencies. Recent legislation in each of the Five Eyes countries has considerably extended information-sharing practices. Across the Five Eyes alliance, cyber-security appears to be a high priority for government and integrated information sharing is argued to be a necessary approach in countering cyber-terrorism. Consequently, a notable legislative trend across the Five Eyes is the implementation of increased intelligence and law enforcement powers geared towards combating cyber-attacks.

All of the Five Eyes nations have experienced similar barriers to sharing and accessing information that have contributed to tragic situations in each of the countries.[5] Consequently, their governments have continued to restructure their security and intelligence communities to foster more effective and cooperative information sharing to strengthen national security efforts. It is recognized that this coordination can help analysts efficiently piece together a pattern of evidence to better detect threats to security and reduce intelligence failures (Collins, 2002). While extending information sharing practices, government authorities across the Five Eyes have simultaneously maintained that they are committed to striking a balance between sharing information and safeguarding private information in respect of civil rights. However, legitimate concerns over privacy rights violations are raised by legal experts, civil rights organizations, and academics in each of the countries. There appears to be resounding agreement that information sharing practices among the Five Eyes intelligence and security agencies are substantially lacking in oversight and review.

With the implementation of the *ATA* and the *SCISA Act*, Canada's information sharing practices are becoming more comparable to the nearly unrestrained sharing US and UK agencies have been employing for years. This has led to similarities in the challenges their respective legislation have faced. While information sharing can be important under times of national security threats, the criticisms of *SCISA* raise

[5] The 9/11 attacks in the US, the 7/7 bombings in the UK, the Canadian Air India Flight 182 bombing, and Australia's failures in the 2002 Bali attacks have all been criticized for government information sharing failures.

legitimate concerns. The potential risks and implications for Canadian citizens who have their information shared and exposed across various government institutions and possibly even foreign bodies are significant. Although the changes introduced in Bill C-59 take initiative to provide further clarity, the changes do not fully resolve these concerns. As well, the consequences of sharing information to foreign governments can have long-term detrimental effects on individuals, as evidenced in the case of Maher Arar and the subsequent Arar Commission Report (2006; Roach & Forcese, 2015a). Preventing incidents such as the Arar case should be a chief concern for the Canadian government. These types of devastating government errors can foster serious public distrust about government activities, subsequently weakening national security strategies (Diamond, 2007). Moreover, SIRC has previously determined that CSIS has mismanaged information sharing with foreign entities. SIRC found certain instances where CSIS had not properly assessed the risks associated with sharing certain information (Tunney, 2018b).

In conclusion, even with the reforms enshrined in Bill C-59, the government has not adequately fixed issues related to information sharing. In fact, it has only changed the term “sharing” to information disclosure, meaning that government is only able to disclose previously held personal data between its government agencies. Moreover, information sharing was only further refined so that data need only be “relevant” to an agency’s operations. This is still too broad and open to subjective perceptions of what private information an agency could deem “relevant” to their operations. It is suggested that the government still needs to restructure its information disclosure structure and clarify when it is “relevant” for each agency to acquire citizens personal data. For example, when is it relevant to share citizens private information to Health Canada in order for the agency to conduct its national security responsibilities? The agency should have to show how obtaining private information is not only relevant but also **necessary** and with no other way to fulfill its responsibilities. In addition, it is suggested that legislation name not just the agencies that can obtain private information for national security purposes, but also the sections of the agencies mandate that pertain to national security to provide further clarification of when accessing citizens personal information is relevant and necessary.

Another way to manage the disclosure of citizens private information so that it does not contravene privacy rights would be to have a single centralized government

agency that reviews, decides, and facilitates the disclosure of data. Under this structure, this expert administrative agency would be mandated with determining when personal information should be disclosed to an agency due to its responsibilities that are directly tied to national security. This would also help oversight bodies by having one main source to review that has a standardized practice of how to it determines the relevancy, necessity, and process through which information is shared between agencies. This would be similar to the US institution known as the Office of the Director of National Intelligence. This institution works to improve intelligence integration by ensuring relevant information is disclosed to each of the US intelligence community agencies (Office of the Director of National Intelligence, n.d.). This goes a step further than simply having a structure in place that allows information disclosure, as it works to ensure private information is going to the right place. Additionally, members on this type of body could be appointed long-term by the Senate, rather than chosen by the Prime Minister, so that it remains impartial rather than vulnerable to changes in government leadership.

Bill C-59 does provide a step in the right direction by improving Canada's national security oversight with the implementation of the National Security Intelligence and Review Agency (NSIRA). The purpose of this committee is to help ensure information sharing is conducted responsibly and in compliance with Canadians guaranteed *Charter* rights. The creation of this committee now aligns Canada with Australia and New Zealand in having an overarching oversight body - a necessary measure to engender public confidence in government activities. However, NSIRA still has weaknesses that need to be addressed before it can truly foster a stronger, more accountable security and intelligence regime. It is essential for government information sharing to be matched with effective review and accountability.

To effectively complete its mandate, it is recommended that NSIRA be provided further authority and resources to ensure privacy rights are being safeguarded. Given the degree of information government can collect and the various agencies this data can now go to, there needs to be an oversight body capable of monitoring the flow of data. This could be better improved by widening the committee so that it has enough staff to investigate agency data-sharing. This also requires respect and cooperation with NSIRA investigations by government agencies. Thus, NSIRA should have the power to gather evidence without government having the ability to block their investigation (which, currently the government has the power to do). This undermines the power of the

committee and does not engender confidence that the group would be able to investigate the most problematic cases.

A second recommendation to improve NSIRA would be to have Parliament elect members, or at least have the ability to challenge nominations made by the Prime Minister. As members are currently chosen by the Prime Minister, this could lead to views that the committee is biased with members being too close to the Prime Minister or having been chosen as they won't ask difficult or probing questions. The UK has also explored ways to improve independency and authority of its intelligence oversight committee by appointing an Opposition member as the Chair of the committee and diversifying members, rather than simply electing former Defence and Foreign Affairs leaders to the committee. This allows for a more balanced committee who will provide different opinions and ensure decisions are not simply made along party lines. These are two viable options the Canadian government should consider when forming this increasingly important oversight body.

4.3.3. Canada's Passenger Protect Program – Secure Air Travel Act

Canada

Air India Flight 182 and the events of 9/11 served as catalysts in the expansion and strengthening of aviation security measures in Canada over the last three decades. The Canadian Passenger Protect (PP) program is the most notable aviation security measure enacted by the Canadian government. The PP program was implemented in 2007 under the *Aeronautics Act* (Public Safety, 2015b). The PP program involves the collection and disclosure of sensitive personal information between Transport Canada, the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS). The core of the program is the Specified Person's List, more often referred to as the "no-fly list" (Public Safety, 2015b). The no-fly list is used as a screening tool to prevent and restrict listed individuals from boarding an aircraft. Airline carriers are required to screen passengers against the no-fly list and an individual who is listed will: undergo further screening processes before travelling, be denied travel by air, or be detained by foreign officials (Public Safety, 2015b). The PP program is also a secretive program, meaning identified individuals are not made aware of their designation on the list. Moreover, government and airlines cannot confirm or deny

listings (Office of the Privacy Commissioner of Canada [OPCC], 2009). This covert process is intended to monitor, prevent, and halt individuals suspected of terrorist involvement from boarding an aircraft. In doing so, Transport Canada aims to "improve aviation security by reducing the threat of terrorism and other criminal acts on flight to or from Canada" (OPCC, 2009, "Introduction").

Since the PP program's introduction in 2007, its functions and procedures have been convoluted and criticized for lacking a firm legal basis. In 2009, the OPCC completed a major audit of the PP program and found several procedural deficiencies. The audit determined the Minister of Transportation was not always provided with complete information on individuals when determining whether to place them on the no-fly list (OPCC, 2009). Additionally, Transport Canada did not monitor whether airlines were complying with no-fly list security measures, and the airlines were not required to report security breaches of personal information (OPCC, 2009). These are major concerns, as placing an individual on a no-fly list has long-lasting impacts on a person trying to travel both domestically and internationally. Additionally, in no circumstance should a breach of personal information not be reported. This entirely undermines confidence in government process and citizens have a right to be informed if their privacy is unduly breached.

Despite ongoing controversy over the Canadian PP program and no-fly lists, Part 2 of the *ATA* provides a firm legal footing to these travel security measures through the enactment of the *Secure Air Travel Act (SATA, 2015)*. The *SATA* (2015) framework outlines significant amendments to the PP program with the primary goal of deterring individuals from departing Canada to promote or engage in terrorist-related activity abroad. The development of *SATA* has emerged from the government's growing concern over radicalized individuals, especially youth, travelling abroad to engage in foreign conflict, often referred to as "foreign fighters" (Public Safety, 2014). The no-fly list is established by the Minister of Public Safety and Emergency Preparedness, who also determines the actions to be taken if these individuals attempt to travel by air (*SATA*, 2015). With the adoption of *SATA*, the threshold to place an individual on the no-fly list was lowered substantially. The Minister only requires "reasonable grounds" to suspect an individual will "engage or attempt to engage in" activity that poses a security threat or is travelling by air to commit a terrorism offence [*SATA*, 2015, s.8(1)(a)(b)]. This threshold is extended to individuals who are reasonably suspected to be flying abroad

with the purpose of participating or contributing to a terrorist group or activity, facilitating a terrorist activity, or committing a terrorist activity [*SATA*, 2015, s.8(b)(i)(ii)]. Moreover, *SATA* authorizes the Minister to disclose personal information of listed individuals to air carriers and foreign governments (*SATA,* 2015, s.12, 13).

The codification of this system is highly problematic. Civil rights and legal organizations have outlined various concerns and weaknesses of *SATA,* emphasizing the procedural flaws (Amnesty International, 2015; BCCLA, 2015; CBA, 2015). In particular, concerns have been raised over the standards in which the Minister can list an individual. The CBA (2015) argues the expanded grounds and lowered thresholds enabling the Minister to list an individual are unprecedented, allowing decisions to be made on "unknown and untested criteria" (CBA, 2015, p. 19). Additionally, the Minister is in charge of self-reviewing and is only obligated to amend the list every 90 days. This process is held in secret and lacks an expeditious process for those individuals denied flight and experiencing urgent circumstances, including medical urgency and compassionate grounds (CBA, 2015).

The most notable concern of *SATA* (2015) and the entrenchment of the no-fly scheme is the lack of transparency surrounding the appeal mechanism outlined in section 16. Despite the right to appeal placement on the no-fly list, section 20 prohibits the disclosure of the list and the associated reasons for placing an individual on the list (*SATA*, 2015). Thus, listed individuals who experience additional screening or denied travel are not entitled to the information explaining why they were listed in the first place. These circumstances make it near impossible for an individual to dispute the information provided to the Minister (CBA, 2015). Within the appeal process, the presiding judge can also hear and rely on evidence that remains undisclosed to the applicant, if the information is opined to be "injurious to national security or endanger the safety of any person if disclosed" [*SATA,* 2015, s.16(6)(c)]. Additionally, information or evidence that would normally be inadmissible in a court of law can be taken into consideration by the judge [*SATA,* 2015, s.16(6)(e)]. Under these appeal provisions, CBA (2015) argues the applicant is at a severe disadvantage in contesting the allegations held against him or her.

The BCCLA also questions the ethics in allowing the government to share no-fly list information with foreign countries but not with the listed individuals (Cheung, 2015). It

remains unclear how this information will be used, managed and safeguarded by foreign countries once shared (Cheung, 2015). The case of Canadian citizen Maher Arar and the subsequent Arar Commission highlights the serious harms that can occur as a consequence of sharing no-fly list information with foreign governments (Roach & Forcese, 2015a). In 2002, prior to the implementation of the PP program in Canada, Arar was arrested, renditioned, and tortured after being stopped in a US airport and deported to Syria due to unsubstantiated suspicions of terrorist involvement (Sallot, 2009). Critics maintain the extreme case of Arar could easily re-occur under the expanded *SATA* provisions (Roach & Forcese, 2015a).

The national security consultation results also demonstrated that Canadians took issue with the current no-fly list procedures under *SATA* and were skeptical of its effectiveness, calling for the process to be reviewed to avoid false positives and an amended clear appeal process for listed individuals. With regard to the changes made in the *SCISA*, participants called for vague definitions to be revised and clearly delineated within the *Act*. It was further suggested that a record of disclosure under *SCISA* should be kept to ensure accountability.

The concerns over *SATA* were slightly addressed in Bill C-59 but still require major amendments to satisfy the problems with false positives and the appeal process. Two major fixes that Bill C-59 does introduce include allowing parents to find out if their children are *not* on the no-fly list and rather than the 90 day benchmark, the Minister has 120 days to respond to any appeals by listed individuals. While these changes are relatively minor, the Liberal government announced in the February 2018 federal budget that $80 million would be put towards revising the system to develop a more “rigorous centralized screening model” and redress system (Tunney, 2018a). Critics are emphasizing that the upcoming review should specifically focus on revising the threshold to list an individual and the secretive appeals proceedings. Specifically, it is being recommended that a special advocate should be allowed to see the evidence held against the individual in order to defend the appellant (Forcese & Roach, 2017).

US

Canada’s PP program shares many similarities with the aviation security program operated in the US. The US Secure Flight program was initiated a mere six weeks after the events of 9/11 by the Department of Homeland Security (2012). The program

includes a no-fly list that is intended to strengthen the security of air travel into, out of, and within the United States (Department of Homeland Security [DHS], 2012). The Secure Flight program is codified through the *Intelligence Reform and Terrorism Prevention Act 2004*. Personal information is collected by the Transportation Security Administration (TSA) and screened against federal government watchlists; TSA personnel have the authority to halt and conduct enhanced screening on listed individuals or prevent them from boarding an aircraft altogether (DHS, 2012). Individuals on the no-fly lists are screened by the FBI's Terrorist Screening Center to establish their travel status (DHS, 2012). The Secure Flight program originally kept the no-fly lists classified, where even listed individuals are not informed of their assignment. This feature and the covert nature of the Secure Flight program parallels Canada's PP program.

The Secure Flight program is criticized extensively by the American Civil Liberties Union ([ACLU], 2015). The ACLU (2015) argues individuals can experience adverse and sweeping consequences due to placement on the no-fly watchlists. This organization maintains no-fly lists expose individuals to discriminatory harassment, detention, and indefinite air travel bans without due process. Moreover, the ACLU (2015) contends the redress process is largely ineffective in allowing individuals a fair opportunity to dispute their placement on the list and clear their names. The procedural criticisms of the secretive functioning and unjust redress process of the Secure Flight program echo many of the concerns raised against the PP program in Canada.

Interestingly, while the Canadian government continues to further entrench strict travel security measures into law, the US government is beginning to take steps to revising the secrecy of its no-fly lists ("The US moves forward," 2015). The Department of Homeland Security Traveler Redress Inquiry Program (DHS TRIP) allows individuals to inquire about or dispute travel bans. In 2014 and 2015, two federal courts ruled the DHS TRIP process failed to provide individuals due process when banned from travelling by air, impeding their constitutionally-protected liberties (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). Both judges ruled the DHS TRIP procedures were considerably flawed, citing the low evidentiary standard of reasonable suspicion that allowed individuals to be placed on the no-fly list and the one-sided nature of the redress process (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). These two court rulings led the US government to restructure its redress procedures (Hunter, 2015).

The newly revised procedures outline that individuals who have been denied boarding an aircraft will now receive a letter indicating their status on the no-fly list (Hunter, 2015). The listed individual will have the opportunity to receive further information and specific details regarding their status (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). This will include an unclassified summary of the information used to determine their placement on the list, except in extreme circumstances where sharing this information will threaten national security. Individuals will be able to utilize this information to dispute their status and request to be removed from the no-fly lists (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). The Administrator of the Transportation Security Administration will review the submission and provide a final determination. If kept on the list, individuals are still granted the opportunity to seek judicial review of this decision (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). While TSA appears to be taking major steps towards revising the classified functioning of no-fly lists, ACLU (2015) argues the redress process still lacks fairness by not providing proper notice, evidence, and a hearing for listed individuals.

UK

In 2012, the UK government implemented the Security and Travel Bans Authority-to-Carry Scheme under section 124 of the *Nationality, Immigration and Asylum Act 2002 (Authority to Carry) Regulations 2012*. The Authority-to-Carry Scheme was invoked with the goal of conducting "pre-departure checks to better identify people who pose a terrorist threat and prevent them from flying to or from the UK" (Home Office, 2012, "Detail"). The Scheme involves an integrated approach between the Home Office, the Department for Transport and UK Visas and Immigration. The Authority-to-Carry Scheme requires airline carriers to check passengers information against watchlists operated by UK Border Agency services. A distinct aspect of this Authority-to-Carry Scheme is the listing of specific foreign nationals under section 124 who could be refused entry to the UK[6] (*Nationality, Immigration and Asylum Act 2002 (Authority to Carry) Regulations,* 2012).

[6] European Economic Area (EEA) nationals with an exclusion or deportation order on grounds of public security, third-country nationals with an exclusion or deportation order on grounds of national security, third-country nationals refused a visa on grounds of national security, or individuals listed and restricted to travel by the UN or EU due to association with Al Qaeda or Taliban.

The UK government recently broadened and further codified national security legislation designed to respond to "the changing terrorist threat" (Home Office, 2014). The 2015 *Counter-Terrorism and Security Act* implemented several prominent security measures with the intentions of "preventing and disrupting the exit from or entry to the UK of individuals posing a terrorism-related threat; and mitigating the threat of an attack on an aircraft operating to the UK" (Home Office, 2014, "Top Lines"). The Authority-to-Carry Scheme was amended and now applies to all individuals, foreign nationals and British citizens, who are suspected of a terrorist-related threat and expected to arrive or depart from the UK (Home Office, 2015). Furthermore, the scheme may specify an individual or even a "class of person…if it is necessary in the public interest" [*Counterterrorism and Security Act*, 2015, s.22(3)]. As well, the Home Secretary is granted authority to impose a Temporary Exclusion Order (TEOs) on individuals reasonably suspected of involvement in terrorist-related activity. The imposition of a TEO can invalidate a British passport and prevent an individual from returning to the UK for up to two years (Home Office, 2015). The *Counter-Terrorism and Security Act* (2015) also extends the Authority-to-Carry Scheme to maritime and rail carriers operating into and within the UK.

The UK government has faced adamant opposition to the legislative changes made to the Authority-to-Carry Scheme. The National Council for Civil Liberties ([NCCL], 2014) specifically contests the ability to target classes of people. It is argued this type of stereotyping will result in serious discrimination and marginalization of targeted groups. Moreover, NCCL (2014) maintains individuals suspected of travelling for terrorist-related activity should not have their passports seized and restricted from travelling. Instead, the NCCL (2014) posits a more effective response is to have carriers notify authorities that a suspected individual intends to travel. This will facilitate appropriate measures, such as surveillance, investigation, or arrest. NCCL (2014) suggests outright denial of travel is not the answer in managing suspected individuals. Instead, the more appropriate response is to deal with suspected individuals through the criminal justice system, rather than forcing the individual to remain in a country (NCCL, 2014).

The UK model is too extreme, and is not one that Canada should follow. Targeting "classes of people," with the ability to refuse entry to an entire group of people based on nationality, is a discriminatory practice that should not be mandated as it directly contravenes values of equality in a democratic country. It is troubling that the UK

can apply decisions based on nationality. This type of discriminatory policy could potentially be extended into basing such decisions on religion, gender, ethnicity, or age. Refusing to allow entry back into one's home country based on potentially unreliable or incorrect information is also an unacceptable practice that Canada should avoid. This can force individuals into dangerous situations, where they may be subject to extreme interrogation or detainment if unable to fly. For example, a citizen who is forced to remain in North Korea due to "suspicion" will experience significant challenges in getting this decision reassessed, and may find themselves subject to extreme detainment conditions. While individuals who present a genuine danger should be stopped during travel as a way of preventing terrorist activity, they should also be properly investigated. At a minimum, this enables errors, such as false positives, to be remedied more efficiently, and steers towards ensuring valid grounds are being applied to stop and detain an individual suspected of travelling for the purposes of engaging in terrorist activity. This highlights a part of the national security framework where both due process and measures to combat terrorism need to be better balanced.

Australia

National security efforts in Australia also focus on enhancing secure aviation measures (Koc-Menard, 2006). Australia implemented the Advance Passenger Processing (APP) system in 2003. The APP mandates airline carriers to provide passenger information to the Department of Immigration and Citizenship (DIAC). This information is checked against Australia's immigration databases, including a Movement Alert List, and passengers may be denied access to air travel (Koc-Menard, 2006). Identical to the rest of the Five Eyes aviation security measures, the APP system aims to identify high-risk individuals and strengthen border security through a pre-emptive strategy. The APP system was recently amended with the enactment of the 2014 *Counter-Terrorism Legislation Amendment (Foreign Fighters) Act.* The APP system originally only applied to passengers bound to Australia but now applies to outbound passengers under the new amendments. This system also applies to international and domestic travel. Further, the APP system applies to ship voyages departing from Australia [*Counter-Terrorism Legislation Amendment (Foreign Fighters) Act,* 2015, s.245LA(1)].

Airline Liaison Officers are mandated to profile travelers and determine whether the individual will be granted permission to travel either inbound or outbound (Koc-Menard, 2006). If an individual is denied permission to travel, the reasons for this decision are kept classified. Keeping these reasons classified aims to minimize "the risk of exposure of intelligence sources and methods" and protect passenger's private information from being shared with the airline carrier and airline personnel (Koc-Menard, 2006, p. 221). However, the APP system does have an appeal procedure and allows for a refusal decision to be overridden. This process is resolved through the DIAC's Entry Operations Center (EOC). The EOC may confirm or overrule the decision to refuse travel after additional checks (Koc-Menard, 2006).

Critics of the APP system suggest this approach utilizes "social sorting," where individuals from "suspect" nationalities are subject to closer scrutiny by Australian processing officials (Wilson & Weber, 2008, p. 130). This is because Australia issues electronic travel authorities (ETAs) to favored nationalities with low recorded risk profiles. Indeed, the APP system has been criticized for targeting individuals on the basis of nationality and ethnicity, especially for asylum seekers who are then subjected to "criminal-justice-like procedures" (Wilson & Weber, 2008, p. 132). It is suggested the expansion of the APP system, along with other tough Australian border security measures, are a move towards punitive and unconstrained surveillance and preemptive national security measures (Wilson & Weber, 2008).

Examining the APP and taking the above criticisms into consideration, it is agreed that Australia's current structure brings up questions of social injustice. This type of system is discriminatory towards those from specific nations, and too closely mirrors racial targeting, by deeming individuals as "suspect status" based on being from a country deemed "high risk." This permits an unjust process where individuals from certain nationalities are subject to greater scrutiny and unequal treatment. This is particularly troubling for refugees seeking asylum who may be forced to return to danger if deemed "suspect status." Further how is a nation determined to be "high risk"? Are these due to a government's political decisions or deals with allies? The ability to deem someone as suspect due to their national origin also allows for the formation of individuals into an elite and lower class based on government decisions.

Moreover, it is concerning this could lead to the acceptance of practices such as applying a risk level to an individual based on ethnicity, descent, birth date, or gender. While screening passengers is indeed a part of ensuring safe flights and monitoring individuals intending to travel for terrorist-related purposes, the ability to create criteria based on being from desirable or undesirable nations should not be a part of the process and is a departure from democratic values, including equality before the law.

New Zealand

In 2003, New Zealand initiated a near identical system to Australia with the Advance Passenger Processing (APP) system (New Zealand Ministry of Affairs [NZMA], 2003). The APP system has been subsequently codified in the *Immigration Act 2009.* Currently, the New Zealand system only requires APP checks on passengers travelling to New Zealand and is not applied to those departing from New Zealand. This information is screened against border security databases and checked against warning lists of persons suspected as threats to national security (NZMA, 2003). The Chief Executive of the Department of Labour decides if a person may or may not board a craft to travel to New Zealand (*Immigration Act,* 2009). If the Chief Executive denies an individual permission, the airline carrier is notified. However, the Chief Executive is not obliged to provide their reasons for the decision to deny entry [*Immigration Act,* 2009, s.97(5)]. Furthermore, an individual denied travel to New Zealand may not appeal the decision, unless he or she is: a New Zealand citizen with a valid passport or a foreign passport indicating New Zealand citizenship; a New Zealand citizen with a foreign passport containing a returning resident's visa; or a resident visa holder with the exception of an individual who has not previously travelled to New Zealand [*Immigration Act*, 2009, s.97(4)].

Conclusions and Recommendations

Several themes emerge when comparing the aviation security measures implemented by Five Eyes governments. In each of the Five Eyes, the national security strategies emphasize the necessity of proactive security measures to forestall, disrupt, and prevent terrorist activity before it occurs. Consequently, the main purpose of implementing no-fly schemes is to better identify individuals suspected of terrorist-related activity and prevent them from travelling by air. The expansion of no-fly schemes

and strict mobility measures are justified as crucial measures to manage the growing concern over homegrown terrorism and foreign fighters.

Overall, the UK appears to hold the most punitive transportation security measures aimed to prevent and manage terrorist-related activity. With the passing of new legislation in 2015, these measures are extended beyond airlines and apply to maritime and rail carriers. Under these changes, individuals denied transportation could be stranded in a country for up to two years (*Counterterrorism and Security Act*, 2015). Moreover, the UK Authority-to-Carry Scheme can be applied to entire categories of people – an unprecedented legislative feature among the Five Eyes. Still, with the adoption of *SATA* (2015) and in comparison to the rest of the Five Eyes, Canada has embraced considerably stringent and covert travel security initiatives. While not as extreme as Canada's PP program, no-fly schemes in Australia and New Zealand appear to be moving towards tougher air security measures.

Overall, the measures outlined under *SATA* (2015) and Canada's no-fly scheme most closely resemble the original US Secure Flight program. However, the appeal process for Canada's no-fly program is much more covert and difficult when compared to US procedures. As indicated, recent amendments to the Secure Flight program require the US government to notify individuals of their placement on the no-fly list. Additionally, individuals are provided an unclassified summary of information as to why they were assigned to the no-fly list. These changes resulted from two prominent US court decisions, determining the appeal procedure violated constitutionally protected mobility rights (*Latif v. Holder,* 2015; *Mohamed v. Holder,* 2015). The CBA (2015) outlines Canada is likely to experience similar court challenges to the appeal mechanisms of the PP program. Despite slight variation in how the no-fly schemes operate in each of the Five Eyes, the criticisms held over no-fly lists are near identical. Most notably is the resounding opposition to the covert nature of the watchlists and air security programs. It is argued the programs lack sufficient judicial and regulatory oversight as well as inadequate redress mechanisms.

Although no-fly schemes are criticized in a variety of ways, no-fly lists can contribute to public safety by securing safe air travel and monitoring individuals suspected of travelling for terrorist-related purposes. Nevertheless, the process of how individuals can address their placement on no-fly lists needs to be redesigned as it is

clearly fraught with concerns. This is necessary, considering being placed on a no-fly list could have immense repercussions for an individual especially if this list is shared with foreign governments. This could include delay or interrogation each time an individual travels both domestically and internationally. We have also seen more extreme cases, such as Maher Arar, which have resulted in individuals being detained and tortured in other countries.

The no-fly list structure is one area of Canada's national security framework that should be restructured from the ground up. Given that the PP program was devised 10 years ago and is wrought with controversy, it is unclear why the government went forth and codified this process into law through the *ATA*. The Liberal's Bill C-59 made little effort to address such issues and the problematic elements remain in place. That said, the Liberal government has pledged that they will dedicate $80 million over the next five years to try and fix the system. Hopefully this process will follow the recommendation provided and aim to innovate an entirely new no-fly list rather than just modifying Canada's dated, flawed system.

Without reform, some improvements could be made to the legislation as it stands. Individuals banned from air travel and seeking redress should have the right to a fair trial, and thus be provided a fair appeal process to dispute their placement. To achieve this, it is recommended that individuals be entitled to a summary of information outlining the reasons for denied travel. This could follow a similar process to the recent procedural changes made to the US Secure Flight program. However, it is understood there may be exceptional situations where the release of this classified information may cause a threat to national security. Under these circumstances, additional independent review of the Minister of Transport's decision could be conducted to ensure the information is factual and reliable. To guarantee due process rights, the appeal process should also provide individuals a timely hearing process. Moreover, if individuals are being watchlisted for simply sharing a name with a suspected terrorist, it is recommended that birth dates be a part of the process. Birth dates are already provided during air travel, and this would at least manage the issues with children being swept up into watchlists.

Additionally, it is recommended the government address the broad language used in specific provisions of *SATA*. Sections 12 and 13 of *SATA* (2015) fail to

adequately explain the necessity in sharing citizens' personal information to foreign countries. It is vital for *SATA* legislation to specify and outline the boundaries of information sharing with foreign countries. A clear framework is necessary in order to understand how individual's personal information will be secured and managed once distributed. Without the above changes, *SATA* and the accompanying amendments to the PP program continues to be problematic.

While not a part of Canada no fly list regime, the fact that countries such as the UK and Australia are nearing practices of social sorting – deeming individuals as "high" risk due to their nationality – is a particularly troubling and discriminatory trend. It is problematic enough that individuals are being put on no-fly lists based on sharing a name with a watch listed individual. Having the ability to determine an individual's flying risk based on nationality would have sweeping repercussions and could be expanded into risk assessments involving age, gender, ethnicity, or colour. It is recommended that government communicate the criteria by which an individual can be watch listed to ensure no decisions are based on unjust criteria, such as nationality, are being employed by government. For those watchlisted, reasons for denial of travel would also engender confidence that discriminatory practices are not being used in Canada.

4.3.4. Expansion of CSIS Mandate and Powers

Canada

The *ATA* implements significant reform to the *Canadian Security Intelligence Service Act (CSIS Act) 1985* by expanding the powers granted to CSIS. These new powers enable CSIS to go beyond information gathering and take disruptive measures to "reduce threats to the security of Canada" [*CSIS Act,* 1985, s.12.1(1)]. CSIS is able to take such measures if there are "reasonable grounds to believe a particular activity constitutes a threat to the security of Canada" [*CSIS Act,* 1985, s.12.1(1)]. While the broad threshold for these measures are to be "reasonable and proportional," the legislation does not outline or define the specific disruptive measures CSIS is authorized to employ. The government and CSIS will decide unilaterally what measures meet this threshold (Forcese & Roach, 2015a). As well, the disruptive measures are extended to include kinetic powers, allowing CSIS to intervene physically with citizens and events, both "within and outside of Canada…" (*CSIS Act,* 2015, s.12.1). Under these measures,

CSIS can go beyond Canadian borders and engage in intrusive activities that cross international jurisdictions. The new kinetic powers are limited to exclude actions such as causing death or bodily harm, willfully attempting to obstruct, pervert or defeat the course of justice, or violating the sexual integrity of an individual" [*CSIS Act*, 1985, s.12.2 (a), (b), (c)]. Allowing CSIS to take measures outside of Canada is deemed necessary to effectively investigate and track Canadian citizens suspected of engaging in terrorist activities abroad (Robertson, 2014). With the introduction of disruptive and kinetic powers to CSIS's mandate, the civilian intelligence agency is capable of offensive action, a power traditionally granted to Canadian police agencies (Collins, 2002).

Additionally, the *ATA* enables CSIS the ability to apply for a judicial warrant to take measures that directly contravene a protected *Charter* right (*Canadian Charter of Rights and Freedoms [Charter],* 1982). It is important to note, CSIS is not required to obtain a judicial warrant for measures that *may* infringe *Charter* rights [*CSIS Act,* 1985, s.12.1(3)]. The government emphasizes the expansion of CSIS powers is necessary to engage in preemptive intervention to disrupt terrorist-related activities, such as suspected terrorist schemes, travel plans, financial transactions, and shipments of material to extremist groups abroad ("New CSIS powers," 2015).

Critics of the reformed CSIS mandate argue these extended capabilities are excessive and injurious to the fundamental values of Canadian society. Particularly, there is adamant opposition to the ability of CSIS to supersede fundamental *Charter* rights through judicial warrant (CBA, 2015; Forcese & Roach, 2015a). It is argued the undefined disruptive measures CSIS is now authorized to employ are essentially limitless and unprecedented (Forcese & Roach, 2015a). As the bill explains, a Federal Court judge is responsible for reviewing CSIS's proposed actions and determining whether there are reasonable grounds to authorize the violation of a *Charter* right. This adjudication takes place through a covert court process. The process is deemed highly problematic, as only the government is represented and judicial decisions are kept confidential and unavailable to the public or the individual being investigated (Forcese & Roach, 2015a). This process severely diminishes public accountability if unjust rights violations occur, as individuals are not able to appeal decisions. The CBA (2015) argues this capability is especially troubling when coupled with the new broad definition of "threats to the security of Canada." The CBA (2015) argues environmental

organizations, indigenous groups, and social or political activist groups may be regarded as “threats,” allowing CSIS to take unrestricted disruptive actions against these groups.

Another main concern over the new mandate is the lack of adequate oversight and review of CSIS activities. CBA (2015) argues there is a severe imbalance between CSIS powers and its oversight and review regime. CSIS’s independent review agency, the Security Intelligence Review Committee (SIRC), has been identified as operating for many years with insufficient resources to effectively review CSIS activities (Roach, 2011). SIRC, already understaffed and under-funded, is now increasingly under equipped to provide sufficient review to expanded CSIS activities. Moreover, SIRC does not have the mandate to oversee all CSIS activity or review other government organizations assisting CSIS in its activities. Accordingly, opponents have called for SIRC’s capabilities to be substantially increased with additional resources and staff, as well as the necessary powers to enforce its decisions (Hall, 2015; Forcese & Roach, 2015a).[7]

The national security consultations held in 2016 resulted in a divide between public opinions on CSIS’ threat reduction powers; some felt CSIS’ new powers should be decreased and others felt they should be maintained. During the forums, these participants often called for CSIS to return to a strictly information gathering agency. Participants cited lack of trust in national security agencies stemmed from their perception that these new powers would allow the government to unduly infringe on Canada’s personal privacy. Participants did agree that safeguards regarding CSIS’ powers need to be significantly increased and that s.12.1(3) be revised to ensure *Charter* rights are never violated (Public Safety Canada, 2017).

Experts have praised Bill C-59 for aiming to reduce the extent of powers provided to CSIS in the *CSIS Act* and clarifies that CSIS is not permitted to cause death, torture, sexually violate, or damage property if it endangers the safety of an individual and even lists measures that CSIS can do with a warrant. Such measures include: altering or destroying communication, records, goods, equipment, fabricating or disseminating

[7] For an extensive analysis of the concerns regarding the new powers granted to CSIS under the ATA, please see: Forcese, C. & Roach, K. (2015d). Intelligence Service’s proposed power to “reduce” security threats though conduct that may violate the law and the Charter. Retrieved from: http://www.antiterrorlaw.ca/

information, making any financial transaction, interfering with the movement of a person, personating a person other than police to take a measure. While there is still controversy among some of the measures CSIS can perform with a warrant, the changes are a vast improvement to ensuring CSIS actions are kept in check and do not permit them to take any action without warrant.

US

The US is well known for its security and intelligence community and their role in undertaking extensive, and highly controversial, monitoring and investigating of domestic and foreign citizens. Although the magnitude of these controversial activities is acknowledged, this analysis will focus on the operational functions of the US intelligence community. The US intelligence community involves an array of intelligence bodies, with the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI) forming the two chief structures (Collins, 2002). The CIA is largely responsible for collecting and analyzing foreign intelligence related to issues of national security (Collins, 2002). This agency has no domestic law enforcement powers and section 3036(d)(1) of the *USC* specifies the Director of the CIA is not afforded "police, subpoena, or law enforcement powers or internal security functions." While the CIA is authorized to perform covert offensive operations, these activities are only permitted in foreign countries. The agency is barred from engaging in covert operations domestically unless, under very limited circumstances, presidential authorization is granted (Forcese, 2015a; Collins, 2002).

The FBI serves as the primary domestic intelligence agency in the US and is responsible for upholding US law and protecting national security (Collins, 2002). While the FBI is mandated with both intelligence and law enforcement responsibilities, it is considered a law enforcement body with police powers. As CSIS is a civilian agency strictly responsible for intelligence, the police powers afforded to the FBI cannot be compared (Forcese, 2015a). Although the scope of CIA and FBI powers are quite extensive, they are explicitly restricted from violating constitutionally protected rights. Executive Order 12333 specifies the covert actions of these intelligence agencies will not be "construed to authorize any activity in violation of the Constitution of statutes of the United States." Comparably, CSIS's new powers surpass the CIA and FBI in its ability to

employ covert domestic action that circumvents citizens rights if approved by a Federal Court judge (Forcese, 2015a).

A few agencies are involved in overseeing the activities of US intelligence agencies. The Director of National Intelligence (DNI) exclusively oversees the CIA and advises the President on their activities (Peritz & Rosenbach, 2009). The National Security Council (NSC) generally oversees the operations of all US intelligence agencies. This oversight and review is conducted to ensure ongoing actions are consistent with national policy and law. However, this review only occurs periodically (Peritz & Rosenbach, 2009). Additionally, the Senate Select Committee on Intelligence (SSCI) is a public, congressional oversight body responsible for reviewing and overseeing the activities of US intelligence agencies.

The intelligence oversight agencies have faced considerable criticism over the effectiveness of their functions for many years. The 9/11 Commission determined the SSCI was highly "dysfunctional" and required significant reforms in order to increase the effectiveness of its oversight functions (Peritz & Rosenbach, 2009). It has been argued these oversight bodies lack objectivity, especially due to the partisan environment in which they operate. Moreover, there have been several incidents where the CIA has been accused of withholding information from these oversight committees and preventing a comprehensive review of the CIA's actions (Mazzetti & Weisman, 2014). There have been strong demands by the public and human rights groups for more effective oversight over US intelligence agencies (Colaresi, 2014). These demands have escalated with growing public awareness into mass surveillance activities and controversial foreign operations employed by US intelligence agencies.

UK

The UK intelligence regime utilizes a twofold system, where the Security Service (MI5) manages domestic national security threats and the Secret Intelligence Service (MI6) manages foreign intelligence and security. The MI5 operates similar to CSIS. This intelligence agency is responsible for countering threats to national security through gathering, analyzing and investigating intelligence information (Security Service, 2015). Conversely, the MI6 is mandated with collecting foreign intelligence and operating covert activities abroad. Canadian government officials posit the new powers granted to CSIS

are analogous to the powers UK intelligence agencies, such as MI5 and MI6, are permitted to carry out (Forcese, 2015a).

This comparison has been highly contested by legal scholars. Forcese (2015a) outlines “neither intelligence service has legal powers to carry out domestic disruption activities involving the breaking of law and the violating of human rights, with warrant or without” (“United Kingdom”). Specifically, the UK *Regulation of Investigatory Powers Act 2000* outlines MI5 cannot conduct investigations violating the *Human Rights Act 1998* (Secret Service, 2015). As well, the MI6 is not authorized to engage in action abroad that would be illegal in the UK. Only under Section 7 of the *Intelligence Services Act*, can the MI6 seek the Secretary of State’s approval in conducting illegal action abroad (Secret Intelligence Service, 2015). However, this exception only applies to international operations and does not allow for such action to be taken domestically (Secret Intelligence Service, 2015). This reveals an important distinction between the new CSIS powers and the MI6. While CSIS can be authorized by a Federal Court judge to take disruptive action within Canada that contravenes constitutional rights, the MI6 can only be authorized to employ this type of action abroad (Forcese, 2015a).

Similar to the US intelligence agencies, the MI5 and MI6 have been heavily criticized for involvement in rendition and interrogation operations over the years (Cobain, Norton-Taylor, & Hopkins, 2013). As well, reports have suggested MI5 and MI6 have withheld information from the intelligence oversight agency, known as the Intelligence and Security Committee (ISC). The ISC, a parliamentarian committee, reviews the activities of all UK intelligence agencies (Security Service, 2015). The implementation of a bi-partisan oversight structure has been praised for offering unbiased supervision of intelligence agency operations (Collins, 2002). However, the committee itself has been criticized for conducting hearings in secret and censoring its reports before publication (Cobain, Norton-Taylor, & Hopkins, 2013). Prominent human rights organizations resoundingly agree the ISC does not have the “independence” or “transparency” to conduct thorough inquiries into the actions of UK intelligence agencies (Amnesty International, 2014, para. 7). Other have suggested the ISC has failed to scrutinize important and controversial intelligence issues on several occasions, including the war in Iraq and the detention and interrogation of terrorist suspects (Bochel, Defty, & Kirkpatrick, 2014).

Australia

The Australian Security Intelligence Organization (ASIO) is responsible for collecting and analyzing information concerning Australia's national security. With the passing of the National Security Legislation Amendment Bill (No. 1 [NSLAB]) 2014, several significant reforms to ASIO were implemented. These reforms closely parallel the new CSIS powers enacted by the *ATA*. Under the 2014 reforms, ASIO officers have been granted the ability to conduct "special intelligence operations" that may contravene Australian law (NSLAB, 2014). Specifically, section 35C outlines ASIO officers are authorized to engage in illegal activity to conduct "an effective special intelligence operation" [NSLAB, 2014]. Similar to the *ATA* provisions, these functions exclude activities leading to: death or serious injury, torture, any sexual offence(s), or serious damage or loss of property [NSLAB, 2014, s.35(c)(e)]. This section goes a step further than the *ATA* provision, which only excludes CSIS from engaging in activity causing death or bodily harm, obstructing justice, or sexual abuse. There is no reference torture will be excluded in the Canadian provisions (*CSIS Act*, 1985, s.12.2 (a), (b), (c)].

Another important distinction between the authority granted to CSIS and ASIO is the Australian law explicitly states ASIO conduct must directly "assist…in the performance of one or more special intelligence functions"[(NSLAB No. 1, 2014, s.35D (1)(a)]. These functions are outlined in section 17(1) of the *ASIO Act 1979* and, unlike the *ATA* provisions, these activities are "aimed at *intelligence gathering"* not "threat reduction" (Forcese, 2015a, "Australia"). Although the new reforms provide ASIO the ability to disrupt computer systems, this disruptive action is restricted to instances where it will "assist the collection of intelligence" [(*ASIO Act,* 1979, s.27E(4)]. Even ASIO's new ability to request a warrant to detain an individual must "assist the collection of intelligence that is important in relation to terrorism offence" and where other methods of intelligence gathering "would be ineffective" [(*ASIO Act,* 1979, s.34F (4)(a)(b)]. Therefore, Forcese (2015a) explains ASIO powers are still restrained to strictly investigating intelligence issues. The reforms to the laws do not extend ASIO's mandate by authorizing disruptive powers as compared to CSIS's new mandate.

Despite these differences and the slightly less radical expansion of ASIO capabilities as compared to CSIS, the Australian government has experienced significant backlash to the ASIO reform (Council for Civil Liberties [CCL], 2014).

Opponents of ASIO's ability to access and disrupt computer systems suggest the broad term of "computer network" allows ASIO to monitor an unlimited number of computers ("Spy laws passed in senate", 2014). Critics of the reform also suggest particular groups will be increasingly under threat, such as journalists or those deemed to be whistleblowers. The CCL[8] (2014) argues the NSLA changes, especially to ASIO powers, have weak safeguards and do not protect fundamental human rights. This is particularly concerning given the absence of a bill of rights in Australia (CCL, 2014). It is suggested the new powers granted to ASIO allow for unnecessary invasion of personal information and violate Australian's privacy rights. Moreover, these groups argue the extension of law enforcement powers to the ASIO is unwarranted and should be left to the Australian Federal Police (AFP) (CCL, 2014).

The NSLA Bill (2014) has also been criticized for providing no means of redress for individuals whose privacy may be affected (MacLeod, 2015). It is the responsibility of the Australian oversight to ensure ASIO is not misusing their powers. The Parliamentary Joint Committee on Intelligence and Security (PJCIS) is Australia's chief intelligence oversight agency. This committee has full access to classified information and reviews ASIO intelligence gathering and operations (Macleod, 2015). This information is reported to Parliament with discovered issues and/or a set of recommendations (Macleod, 2015). The Australian system also utilizes three other oversight and review agencies, including the Inspector-General of Intelligence and Security, the Independent National Security Legislation Monitor, and a parliamentary joint committee on human rights (Macleod, 2015). As well, judicial review is conducted on ASIO-obtained warrants, administrative tribunals and when an independent review of ASIO assessments is required (Macleod, 2015). Despite various oversight agencies, critics suggest these groups do not have the ability to effectively review ASIO activities given the high volume of operations ASIO conducts (Belot, 2014). It is maintained oversight bodies need more staff and resources to keep pace with the increases in authority and personnel to the intelligence agencies (MacLeod, 2015).

[8] Council for Civil Liberties includes: New South Wales Council for Civil Liberties, Liberty Victoria, Queensland Council for Civil Liberties, South Australia Council for Civil Liberties, Australian Council for Civil Liberties, Civil Liberties Australia).

New Zealand

Within New Zealand, the Security Intelligence Service (SIS) is responsible for investigating threats to security, collecting intelligence and providing security advice to the government in order to protect national security. The SIS is required to be an apolitical civilian intelligence and security organization (Security Intelligence Service, n.d.-a). The implementation of the 2014 Countering Terrorist Fighters Legislation Bill led to important amendments to New Zealand's *Security Intelligence Service Act [SIS Act] 1969*. Although the SIS is not permitted to conduct kinetic disruption operations, the amendments allowed the agency to seek a judicial warrant allowing them to undertake visual surveillance on private property (*SIS Act,* 1969, s.41B). However, in "emergency" circumstances SIS can also undertake warrantless surveillance for up to 48 hours (*SIS Act,* 1969, s.41D). These are similar capabilities granted to the New Zealand police force, but SIS does not have disruption powers. In response to changes in Canadian, American, British, and Australian national security legislation, SIS is pushing for more expanded powers to keep pace with the Five Eyes community (Vance, 2015). Although amendments were passed in 2014 expanding SIS powers, the current New Zealand government has announced they will be reviewing SIS functions again with plans to extend their powers (Edwards, 2015). It is not yet known whether these changes will include disruption powers.

Opponents of the expanded SIS powers suggest that the introduction of warrantless domestic surveillance by SIS is extremely intrusive and unprecedented for New Zealand. Critics fear these new powers will be used to target environmental or political activists (New Zealand Law Society, 2015). Indeed, they suggest that the new authority be deleted from legislation. Allowing domestic warrantless operations is argued to be a massive infringement on the privacy rights of citizens (Law Society, 2015; Young, 2014).

The Inspector-General for Security and Intelligence primarily monitors the operations of SIS to ensure that the agency is complying with the proper policies and any actions are lawful and proportionate (Security Intelligence Service, n.d.-a). Oversight and review of SIS operations have experienced similar problems to Five Eyes intelligence agencies. A recent report by the Inspector-General determined SIS failed to disclose certain information to the Prime Minister's Office and other times disclosed

incomplete or misleading information (Gwyn, 2014). This has caused some distrust of SIS in the public eye and raised demand for increased oversight of SIS operations (New Zealand Law Society, 2015).

Conclusions and Recommendations

Across the Five Eyes nations, legislative changes have geared towards increasing the powers of their intelligence and security agencies to protect national security and suppress terrorist activity (Collins, 2002). However, an examination of the domestic powers granted to each country's leading intelligence agencies reveal CSIS's increased capabilities goes beyond any of the other Five Eyes. While the US and the UK allow their agencies to engage in covert disruption activities, which may violate their respective laws, these activities are restricted to foreign operations. Although the CIA can seek Presidential approval to engage in covert action domestically, legislation explicitly states these activities cannot violate any US constitutionally protected rights. The *ATA* allows CSIS to conduct such activities both within and outside of Canada, where a Federal Court judge can approve activities potentially violating *Charter* rights. In contrast, it appears both Canadian and Australian law allow, under certain circumstances, their intelligence agencies to have a degree of immunity from criminal and civil liability. Currently, intelligence agencies in the US, the UK, and New Zealand do not have this type of immunity when engaging in domestic operations.

The reform to ASIO activities to engage in special operations and disruption of computer systems are most comparable to CSIS's new kinetic powers. However, these activities are more extensively outlined and defined in Australian legislation as compared to the broad provisions in the *ATA*. The sections outlining ASIO's activities explicitly outline special operations, detainment, and disruption of computer systems must be directly related to assisting the collection of information. Comparatively, the *ATA* authorizes CSIS disruption if there are reasonable grounds a threat to national security is present, and would likely occur without action. However, changes outlined in Bill C-59 scale back CSIS powers by listing what CSIS threat reduction powers allow them to do and confirming they cannot engage in any type of detainment, torture, or damage of property at the risk of endangering life.

And yet, Bill C-59 still enshrines bulk data collection powers granted to CSIS that were not permitted before the *ATA*. The agency is allowed to collect certain datasets

under the Minister of the Public Safety's authorization if deemed relevant to CSIS performance, as well as any data that is "publicly available," without clarity on the limits of what could be considered public data. For instance, does publicly available data have to be lawfully obtained? While the wording has changed, it seems that CSIS can still obtain mass data. While data collection does not necessarily mean mass surveillance, safeguards are necessary to ensure sensitive data is not exploited and is indeed used for national security purposes. It is recommended that certain criteria be established that outlines what type of large datasets could be collected and the limits on how this data is obtained. Such activity should be subject to intense oversight. Also, it is recommended that data should not be collected if the Minister of Public Safety deems it relevant but should be based on whether the data is necessary to operations. While it could be argued this higher threshold impedes or slows government operations, it is posited that if data does directly pertain to operations, government should have no problem making the case that it is indeed "necessary."

Canada, through the introduction of the NSIC in 2016, now aligns with the UK, Australian, and New Zealand models where parliamentarians are involved with review and scrutiny of national security matters (MacDonald, 2011). Bill C-59 provides a step in the right direction with CSIS now subject to oversight by NSIRA and the Intelligence Commissioner. The concerns previously explained over NSIRA members being elected by the Prime Minister and provided no real power, however, make this oversight system weak. As stated, it is recommended that NSIRA decisions have power to issue remedies rather than just treated as recommendations. Additionally, opposition members should be able to contest members elected or be elected more objective by parliament rather than just the Prime Minister to ensure credible appointees. As well, it is yet to be seen whether this oversight body will have the budget and staff required to undertake the mass operations that CSIS undertakes.

Within each of the Five Eyes, opponents to extending intelligence agency powers express general consensus over the necessary distinction and separation between powers designed for intelligence agencies and law enforcement agencies (Forcese & Roach, 2015a). An agency directly responsible for intelligence should be concerned with collecting intelligence and investigating intelligence issues. Although Bill C-59 refines what actions CSIS can conduct, the responsibility to disrupt or take physical action against these issues should be left to law enforcement agencies. Given CSIS' current

structure as an intelligence body, it is recommended that kinetic powers be left to law enforcement agencies if CSIS remains exclusively as an intelligence agency. Clarity over the division of responsibilities between these two agencies is necessary. Policy developments should work towards strengthening the cooperation between these two agencies and their counterterrorism operations. If CSIS powers are necessary for foreign operations, perhaps there should be a move towards creating domestic and foreign intelligence agencies each with different mandates and powers, similar to the structure found in the US and the UK. For instance, Bill C-59 allows CSIS to collect data on non-Canadians outside of Canada. This type of power seems better suited to an agency that is focused on foreign intelligence. This would have to be a careful consideration in order to not overload CSIS' mandate but rather create a body that would manage foreign intelligence. Foreign operations are more complex given the political, economic, trade, military factors that influence these operations. By having two separate agencies, this could ensure foreign operations are not infecting domestic ones. Currently, CSIS can use "incidental" information passed from foreign governments (Stewart, 2014). However, it is difficult to discern the credibility of this intelligence and thus having a foreign intelligence agency would mean that Canada would partake in its own investigations rather than relying on information passed on from foreign agencies. This is not to suggest the two agencies would work in absolute silos, but instead are clear about the skills, tactics, and legal powers each can use and operate within. Globally, democratic governments have consistently proven that foreign operations can involve aggressive espionage and surveillance that arguably operates outside of what would be allowed for domestic operations. For example, the distinction of power between the FBI and CIA asserts that the FBI cannot take action that infringes on citizens constitutional rights. There is credence then to separating domestic and foreign intelligence operations in order to avoid CSIS actions becoming convoluted and operating outside of what is permitted by the Canadian legal system.

4.3.5. Conclusion: Five Eyes National Security Approaches

The specific provisions implemented by the *ATA* and discussed above provides insight into Canada's current approach to developing a national security framework aimed to combat terrorism. It is important for government officials and citizens to be critical and assess the trajectory of Canada's national security strategy - the *ATA*

resulted in mass public outcry with regards to the favouring of security over citizens' rights. As such, the current Liberal government is attempting to restructure Canada's approach by scaling back some of the controversial measures implemented through the *ATA* and ensuring *Charter* rights are still reasonably protected. In order to achieve a resilient national security strategy while protecting the fundamental elements of a democratic society, it is prudent for policymakers and government officials to try and strike this balance between security and civil liberties in Canadian policy (Freese, 2014). This standard is noted in varying degrees throughout each of the Five Eyes members' national security strategies, however, respective legislation across the countries appears to tip in favor of firm security measures.

Given the shared history and alliance of the Five Eyes network, it is not surprising to find a resemblance between their national security legislation and policies (Cox, 2012). The similar language and overarching goals found within each member's national security legislation and policy demonstrate these measures have been undoubtedly shaped by each other. In the post-911 environment, all of the Five Eyes members have continually restructured and bolstered national security measures, utilizing similar strategies as their allies. The US *PATRIOT Act* was once at the forefront of tough national security strategies due to the sweeping changes implemented in response to 9/11. The Conservative UK government, however, appears to be leading the charge in pursuing extensive and tough national security legislation, which appears to be correlated with their historical and current day experiences with terrorist incidents on home soil (Moran, 2005; Mason & Dodd, 2017). The Australian government has also been increasingly assertive in amplifying the severity of their national security legislation and policy. New Zealand's national security strategy is arguably less severe when compared to Canada and the rest of the Five Eyes members. This is likely due to the evaluation of New Zealand's terrorist threat as low, whereas Canada and the other members have been assessed as varying from medium to high (Security Intelligence Service, n.d.-b; Sinai, 2015; UK Government, 2015; MacLeod, 2015).

Nonetheless, the above analysis of certain controversial provisions does demonstrate that in some areas the Conservative crafted *ATA* does push the boundaries of tough security measures when compared to the other Five Eye members. Changes to Canada's no-fly list make this program more covert than its US counterpart. Under *SCISA,* Canada's information sharing practices between its government agencies has

increasingly expanded similar to UK and Australian levels. Overall, it remains in question whether national security measures implemented by the *ATA* were introduced to genuinely combat "the threat of terrorism" in Canada, or to heighten Canada's stance among its close allies as a leader in national security (*ATA*, 2015). It is argued that the increase in severity of Canada's national security measures has created tension between citizens and government especially where such measures were thrust forward without clear communication by government and without transparency as to how these new measures would be utilized.

Although the *ATA* has undeniably increased Canada's security measures, the Liberal government's Bill C-59 aims to scale back some of these provisions and address public concerns. Although Canada's national security approach is far from perfect, the implementation of the national security consultations is a major step forward to redressing some of the powers granted to government in the *ATA*. Moreover, the Liberals appear to have taken into consideration the results of the consultations where Canadians emphasized their desire for accountability and transparency of government powers along with greater protection of their democratic rights. The current Public Safety Minister, Ralph Goodale, even stated the primary goal of the legislation is "to strike a balance between keeping Canadians safe and respecting their rights and freedoms" (The Canadian Press, 2017). While the bill does not eliminate all powers provided to government through the *ATA,* it makes considerable improvements by introducing more oversight and accountability and providing further clarification over the processes and definitions regarding national security matters. The bill is likely to pass in 2018 but debate over government powers and how to best achieve a balance between security and privacy will continue to dominate public policy conversations.

Despite the challenges posed in comparing policy and legislation across international jurisdictions, there is no doubt Canada and the remaining Five Eyes members are following very similar trajectories when crafting their national security strategies. Each government has reinforced the notion that in order to preserve and protect democracy, national security must be prioritized. An examination into recent government national security strategies demonstrates this emphasis on national security stems from an overwhelming concern over the radicalization and recruitment of extremist supporters and lone actors, homegrown terrorism, and cyber-attacks. While Canadian national security strategies may have appeared benign compared to some of

the measures used by its allies, the implementation of the *ATA* escalated government powers and thrusted Canada into the global debate about the extent of power democratic governments should be allowed to invoke under the guise of national security, and how to ensure citizens safety without unduly impeding on constitutional rights.

Despite the scaling back of the stricter measures implemented through the *ATA*, the government still has not sufficiently contextualized the need for these measures and how they will be implemented in real-life situations. To be sure, it seems that in Canada the government's perceived risk of national security threats is incongruent with that of the public. In order for Canadians to support the legal reach of new or enhanced national security measures, government needs to be able to communicate and provide further information to satisfy the public that such measures have merit. Additionally, due to the sensitive nature of national security incidents, the public is rarely provided with tangible evidence that such measures are being used to effectively combat security threats. Often the public is relying on government's narrative – and this is weakly communicated by simple statements suggesting the government has foiled a recent plot or merely following what other countries have legislated.

This problem can be seen throughout each of the Five Eyes, where many new elements of proposed legislative change are introduced as reactions to a national security incident that has occurred. Rather than explaining how these new measures or legal consequences will be used in various situations going forward, it is argued the new measures and stronger penalties implemented could have prevented that specific incident. This approach could be ineffective, as it is focusing on a past event, and could curtail the government's ability to think about emerging threats and other potential gaps in security. By crafting legislative measures focused on preventing or mitigating a past event, these measures may not be relevant to threats in the future due to changes in conditions. Instead it is argued that a national security framework needs to be proactive rather than reactive in order to effectively respond to unanticipated crisis.

Chapter 5.

Establishing an Effective National Security Strategy in Canada

Significant changes appear to be taking place in how nations view and implement national security strategies. While security was once more focused on addressing foreign threats through military or political processes, governments have widened their view of threats to the nation in the post 9/11 era (Caudle, National Security Strategies). This has had clear implications for policy development. To address this expanded view of threats that undermine a nation's security, governments have continually revised their national security strategies and even crafted entirely new ones. In doing so, however, many governments have implemented measures that conflict with citizen's rights. This has led to debate about whether citizen's rights can be infringed upon to secure safety or to what extent rights can be derogated when striving to develop an effective national security strategy.

Within each of the provisions assessed in Canada and compared to the other Five Eyes strategies, there is validity to concerns raised by the public. Although the exercise of draconian measures to combat complex challenges is not new to democratic societies, specific provisions of the *ATA* are arguably excessive and overstep civil liberties (Forcese & Roach, 2015a). The line between police, intelligence, and security agencies is becoming increasingly blurred in government approaches even with the probable passing of Bill C-59. There remains ample debate that citizens' privacy rights will be increasingly infringed upon due to the expansion of terrorist-related offences, inter-department government information sharing, and expanding powers granted to police and intelligence bodies (Amnesty International, 2015; CBA, 2015; BCCLA, 2015).

Strategies guide a country's plans, programs, campaigns, national and international reputation, and activities when it comes to securing national interests and combating potential threats. Moreover, a national strategy must be adaptable and achieve multiple objectives. It is clear the implications of a country's strategy choices are widespread and significant. In Canada, specifically, government has been struggling to

craft a clear strategy and has resulted in debates regarding views of national security, how it should be secured, what is important to secure, and whether it is the nation or individual citizens' security that should be secured. To work towards developing an effective national security strategy framework, the following section provides recommendations to establish a framework that achieves government purposes and secures public confidence.

It is important for a nation's national security strategy to clearly address the above elements or any action will lack direction and consistency. It is recommended that Canada's national security framework meet the following characteristics. These characteristics can help policymakers ensure their strategies are clear and reflective of a nation's values:

1. Statement of purpose and scope – provide context for initiatives
2. Identify threats and risks they pose
3. Clearly link goals to the objectives of the actions outlined - identify and address potential risks of actions
4. Measures and actions must be subject to oversight
5. Roles and responsibilities of actors and citizens, and prioritization of resources
6. Plan of implementation

Characteristics 1-3 above require policymakers to communicate a strategic vision to inform public about the intent of their strategy and the nation's values. This involves explicit goals and requirements to address identified threats to the homeland. When identifying national security risks, the full range of threats should be made clear and what measurable actions are being taken to address these issues along with any possible repercussions of these proposed actions.

For characteristic 4, it is important for policymakers to review previous policies and legislation related to national security along with *Charter* rights to ensure any new measures are crafted in line with these elements. It is arguably of utmost importance that citizens are assured that their government is crafting a strategy that does not undermine their own rights and freedoms, and conduct sufficient reviews of their actions. If the process underlying a strategy is flawed, it is argued the national security strategy will be

flawed (Doyle, 2007). Additionally, it should be noted that no amount of oversight or review can make up for a flawed strategy.

Lastly, for characteristics 5 and 6 to be met, it requires that the specific roles of all agencies and processes for coordination are explicitly outlined – indicating what elements of national powers are to be used to meet each goal and a clear guide to this process. All these characteristics are imperative to ensure a country's government and citizens have a clear understanding of the goals, threats, and values set out in its national security strategy.

In reviewing Canada's national security approach against these characteristics, it is argued that the current strategy is lacking in characteristic 4-6. Despite changes put forth in Bill C-59, it is argued that the oversight of Canada's national security strategy is insufficient and requires more resources. Governments' increased efforts to strengthen national strategies through legislation and policy need to be matched by robust accountability mechanisms. Without effective review and accountability measures, the countries will fail to gain confidence from the public (Conte, 2010). Additionally, the *ATA* does not explicitly communicate what agencies are involved in certain national security elements or how these agencies coordinate with one another. Canada's national security strategy can be vastly improved by addressing these issues. It is recommended that further substance and clarity be added regarding leadership and accountability in security actions and measures.

Despite these flaws, Canada has excelled in another important feature for a national security strategy to be evaluated against: how it mobilizes the country and its citizens towards shared values. The Conservative government's implementation of the *ATA* mobilized the majority of the public and experts in a negative manner but did motivate the public to become involved in discussions around national security. Many felt the *ATA* and its measures were unnecessary, did not reflect Canada's security values, and was a blatant attack on the rights and freedoms of Canada's own citizens. This served to mobilize academics, civil liberties groups, NS activist groups to speak out against the *ATA.* The involvement of the public and experts resulted in Canada's national security strategy becoming a major campaign topic of the 2015 federal election. This was arguably one of the driving factors that led to the Liberal election win. In turn, the Liberals have kept to their election promise and worked to engage with the public to

better determine what Canadian citizens perceive as threats and what the correct boundaries are for government to address these threats. The National Security Consultations involved the public through a variety of platforms – online questionnaires, public town halls, and expert consultations. These Consultations were a stride forward in mobilizing citizens' engagement in a positive way and helped to determine the Canadian concept of national security and how to better reflect how Canada viewed security and approaches to national security. Although there is still some work to be done to achieve a strategy that is truly reflective of the nation and its citizens, when compared to the rest of the Five Eyes with the exception of New Zealand, Canada has taken a major step forward in respecting the individual when it comes to security.

Chapter 6.

Conclusions and Limitations

National security strategies have received considerable international attention as a result of shocking international terrorist incidents in the post-911 era that threaten regional and global order. Globally, governments have responded by implementing various legal and policy measures aimed to combat terrorist-related activity often within compressed time frames in response to such events (Kossowka, Trejtowicz, de Lemus, Bukowski, Van Hiel, & Goodwin, 2011; Roach, 2011). Crafting these national security strategies are among the most crucial responsibilities of governments and policymakers; these strategies have significant national impacts and sometimes even global impacts. National security strategies outline what government perceives to be threats to the nation and what national interests fall under the umbrella of security. These strategies also demonstrate how government prioritizes goals to preserve national security and the instruments and power they deem necessary to do so. As such, national security strategies can provide insight into how government prioritizes such measures with constitutional rights afforded to citizens in a democratic society.

Despite many countries having implemented sweeping changes and expansions to national security strategies since 9/11, the changes enacted through the *ATA* in Canada are regarded as unprecedented steps that demonstrate a clear prioritization of security over civil liberties (Roach & Forcese, 2015a). Although the Liberal government is seeking to scale back the powers enacted through the *ATA* in their new national security bill, Canada's national security strategy appears to be very much "catching up" with the rest of the Five Eyes in terms of tough security measures with the exception of New Zealand. Additionally, even scaled back *ATA* measures have resulted in Canada's national security regime being extended with more pieces of legislation that are likely to be supplemented further in later years.

Tracing the links between national security strategies among Canada and the Five Eyes provides a systematic account of perceived threats and methods of response. Consequently, this policy analysis allows for a better understanding of the emerging patterns and themes across provisions of Canada's current national security legislation

and similar provisions implemented by the rest of the Five Eyes. While a comparative policy analysis encourages a better understanding of global national security strategies, it is important to note the methodological challenges associated with this strategy. Public policies can be complex entities developed within a country and shaped by its own unique circumstances and history (Engeli & Allison, 2014). Each country operates in a distinct social, political, and economical environments, involving a diverse group of interacting actors and organizations. It is acknowledged that national security strategies are a reflection of current cultural and political principles such as whether nations or their governments embrace liberal and conservative values. Additionally, public policies are developed in order to achieve a certain goal, and these goals and the means to achieve them can vary dramatically from country to country (Engeli & Allison, 2014). One other limitation specific to national security strategies, is the complexity of terrorist events themselves. Such events are often so intentionally erratic and unpredictable that they are nearly impossible for governments to prevent. This greatly hinders the ability to quantify or measure the effectiveness of certain strategies, thus making it a complex and arguably impossible task to determine what measures do or do not work in securing national security and combating terrorism.

Hence, considerable differences in policy-making can emerge due to the country-specific and highly complex environment in which they operate including the presence or absence of an ongoing terrorist threat. This is seen when comparing New Zealand's milder national security strategy with the rest of the Five Eyes which is likely attributed to their lower threat level and lack of recent domestic terrorist incidents. Despite challenges faced when evaluating policies across international jurisdictions, Freese (2014) argues the importance in continuing comparative and evaluative research on counterterrorism efforts. This type of exploration can provide insight into whether policy-makers are using terrorism-related research to assist in the development and implementation of effective national security strategies. Moreover, comparative policy research can help identify the strengths and weaknesses of Canadian and international national security strategies (Freese, 2014).

Additionally, this research could be improved by assessing how the national security measures examined are realistically used among Canada's national security agency's. This can be achieved by conducting interviews with practitioners. Interviews can provide in-depth understanding into how these measures are realistically used and

the feasibility of the recommendations presented. It is possible some of the recommendations provided could be impractical based on practitioner's knowledge of how these agency's realistically operate. Alternatively, interviews could confirm the recommendations suggested. Interviews could also be beneficial in obtaining diverse opinions and views from professionals. This could help develop new or innovative approaches to addressing some of the issues explored in this research.

A series of complex challenges still exist for democratic governments in establishing effective national strategies in the post-9/11 environment (Freese, 2014). Governments must take into careful consideration civil liberties guaranteed to its citizens, while also developing robust legal tools to manage the threat of terrorism, both domestically and abroad (Diamond, 2007). Further, this comparative policy analysis brings forth a series of important issues to be explored in future research. In order to resolve the challenges posed by terrorism, it is imperative to understand the difficult balance between enhancing national security and protecting civil liberties. It has yet to be determined whether democratic governments can prevent or deter terrorism without unduly infringing upon citizens' rights and freedoms (Freese, 2014; McGill & Gray, 2012). As evidenced through this analysis, democratic government's boundaries in developing effective national security strategies are complex and highly debated. Going forward, evaluative research must be utilized to accurately understand the effectiveness of these policies (Freese, 2014). Equally as important, is using evidence-based research as the foundation for future national security laws (Freese, 2014). These considerations are key to achieving good governance in Canada and establishing a resilient national security strategy.

References

American Civil Liberties Union. (2015). *Watchlists.* Retrieved from https://www.aclu.org/isues/- national-security/privacy-and-surveillance/watchlists

Amnesty International. (2015, March 9). Insecurity and human rights: Canada's proposed national security laws fall short of international human rights requirements. Retrieved from http://www.amnesty.ca/news/news-releases/insecurity-and-human-rights-canada's-proposed-national-security-laws-fall-short

Amnesty International (2014). NGO joint letter to the ISA on the detainee inquiry. CAGE. Retrieved from http://www.cageuk.org/article/ngo-joint-letter-isc-detainee-inquiry

Anti-terrorism Act, S.C. 2015 c. 20.

Ashour, O. (2011). Online de-radicalization? Countering violent extremist narratives: Message, messenger, and media strategy. *Perspectives on Terrorism, 4*(6), 15-19. Retrieved from: http://www.terrorismanalysts.com/pt/index.php/pot/article/view/128/html

Attorney General. (2014). *Counter-terrorism legislation amendment (foreign fighters) bill 2014: Explanatory memorandum*. The Parliament of the Commonwealth of Australia. http://www.attorneygeneral.gov.au/Mediareleases/Documents/140923-EMCTForeignFightersBill2014.pdf

Australia. Parliament. Senate. (2014). *National security legislation amendment bill (no.1) 2014: Explanatory memorandum*. Retrieved from http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/s969_ems_2dbf9bb1-59cd-44ed-8e6a d106c5535c72/upload.pdf/396762em.pdf;fileType=application%2Fpdf

Australian Human Rights Commission. (2014). *Submission to Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014.* Retrieved from https://www.humanrights.gov.au/submissions/submission-inquiry-national-security-legislation-amendment-bill-no-1-2014#Heading260

Australian National Security Law. (2017, Feb 7). Legislative Framework. Retrieved from https://ausnatsec.wordpress.com/contact/

Barak-Erez, D., & Scharia, D. (2011). Freedom of speech, support for terrorism, and the challenge of global constitutional law. *Harvard National Security Journal, 2*(1), 1-30. Retrieved from http://harvardnsj.org/wp-content/uploads/2015/01/Vol.-2_Barak- Erez_and_Scharia_Final.pdf

Belot, H. (2014). Intelligence watchdog's oversight called 'weak' as new powers granted to spy agencies. *The Sydney Morning Herald*. Retrieved from http://www.smh.com.au/national/intelligence-watchdogs-oversight-called-weak-as-new-powers-granted-to-spy-agencies-20141014-115qfr.html

Bill 27-2. Counter-Terrorism Bill. (2003). 1st Reading January 4, 2003, 47th Parliament. Retrieved from the New Zealand Parliament website: http://www.parliament.nz/en-nz/pb/legislation/bills/00DBHOH_BILL5176_1/counter-terrorism-bill

Bill C-59: An Act respecting national security matters. (2017). 1st Reading, June 20, 2017, 42nd Parliament, 1st session. Retrieved from the Parliament of Canada website: http://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/first-reading

Bochel, H., Defty, A., & Kirkpatrick, J. (2014). *Watching the watchers: Parliament and the intelligence services.* Palgrave Macmillan. Basingstoke: Hampshire.

British Columbia Civil Liberties Association. *Submissions: Bill c-51, the anti-terrorism act, 2015.* Retrieved from https://bccla.org/our_work/submission-to-the-standing-committee-on-public-safety-and-national-security-bill-c-51-the-anti-terrorism-act-2015/

Burch, J. (2007). A domestic intelligence agency for the United States? A comparative analysis of domestic intelligence agencies and their implications for homeland security. *Homeland Security Affairs, 3*(2), 1-26. Retrieved from https://www.hsaj.org/articles/147

Burgess, M. (2017, May 8). What is the IP act and how will it affect you? *Wired.* Retrieved from http://www.wired.co.uk/article/ip-bill-law-details-passed

Buzan, B., Wæver, O, & Wilde, J.P. (1998). *Security: A new framework for analysis.* Boulder, Colorado: Lynne Rienner Publishers. Print.

Canadian Bar Association. (2015). *Bill c-51, anti-terrorism act, 2015.* Retrieved from http://www.cba.org/CBA/submissions/pdf/15-15-eng.pdf

Canadian Civil Liberties Association. (2018a). National security: Get it right! Retrieved from https://ccla.org/campaigns/c59/

Canadian Civil Liberties Association. (2018b). Ten things you need to know about bill c-59. Retrieved from https://ccla.org/ten-things-need-know-bill-c-59/

Capoccia, G. (2013). Militant democracy: The institutional bases of democratic self-preservation. *Annual Review of Law and Social Science, 9,* 227-226. doi: 10.1146/annurev-lawsocsci- 102612-134020

Caudle, S.L. (2009). National security strategies: Security from what, for whom, and by what means. *Journal of Homeland Security and Emergency Management, 6*(1), 1-29. doi: https://doi.org/10.2202/1547-7355.1526

Cheung, C. K. M. (2015, April 22). Submissions: Bill c-51, the anti-terrorism act, 2015. *British Columbia Civil Liberties Association.* Retrieved fromhttps://bccla.org/our_work/submission-to-the-standing-committee-on-public-safety-and- national-security-bill-c-51-the-anti-terrorism-act-2015/

Cobain, I., Norton-Taylor, R., Hopkins, N. (2013). MI5 and MI6 face questions over torture of terrorism suspects*. The Guardian*. Retrieved from http://www.theguardian.com/politics/2013/dec/19/mi5-mi6-questions-torture-terrorism- rendition

Cohen, Z. (2017, May 26). How US intelligence leaks upset two allies in one week. *CNN.* Retrieved from https://www.cnn.com/2017/05/24/politics/manchester-us-leaks-allies/index.html)

Colaresi, M. (2014, Dec 12). Why the CIA should want more congressional oversight, not less. *The Washington Post.* Retrieved from http://www.washingtonpost.com/blogs/monkey-cage/wp/2014/12/12/why-the-cia-should-want-more-congressional-oversight-not-less/

Cole, D. (2012). The first amendment's borders: The place of *holder v. humanitarian law project* in first amendment doctrine. *Harvard Law & Policy Review, 6,* 147-177. Retrieved from http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1865&context=facpub

Collins, D. (2002). Spies like them: The Canadian Security Intelligence Service and its place in world intelligence. *Sydney Law Review, 24*(4)*,* 505-528. Retrieved from http://www.austlii.edu.au/au/journals/SydLRev/2002/23.html

Conte, A. (2010). Human rights in the prevention and punishment of terrorism. 423-464. *Springer Berlin Heidelberg*. doi: 10.1007/978-3-642-11608-7_14

Council of Australian Governments. (2015). *Australia's counter-terrorism strategy: Strengthening our resilience*. Commonwealth of Australia. Retrieved from http://www.nationalsecurity.gov.au/Media-andpublications/Publications/Pages/dafault.aspx

Counter Extremism Project. (2017). United Kingdom: Extremism & counter-extremism. Retrieved from https://www.counterextremism.com/countries/united-kingdom

Countering Terrorist Fighters Legislation Bill. (2014). New Zealand Government. Retrieved from http://www.legislation.govt.nz/bill/government/2014/0001/21.0/whole.html#contents

Cox, J. (2012). *Canada and the five eyes intelligence.* Strategic Studies Working Papers. Canadian Defense and Foreign Affairs Institute and Canadian International Council. Retrieved from http://opencanada.org/features/the-think-tank/essays/canada-and-the-five-eyes-intelligence-community/

Criminal Code, R.S.C., 1985, c. C-46, s. 22(1), s. 83.21, s. 83.221, s. 319(2)

Cullen, M., & Reddy, D.P. (2016, Feb 29). Intelligence and security in a free society. *Report of the first independent review of intelligence and security in New Zealand.* Retrieved from https://www.parliament.nz/resource/en-nz/51DBHOH_PAP68536_1/64eeb7436d6fd817fb382a2005988c74dabd21fe

Davis, J. (2012, April 26). Ottawa abolishes spy overseer's office. *National Post.* Retrieved from http://news.nationalpost.com/news/canada/canadian-politics/former-csis-officer-warns-new-federal-anti-terror-bill-will-lead-to-lawsuits-embarrassment

Demirsu, I. (2017). Counter-terrorism and the prospects of human rights: Securitizing difference and dissent. Cham, Sqitzerland: Palgrave MacMillan. doi 10.1007/978-3-319-50802-3

Department of Homeland Security. Office of Inspector General. (2012) *Implementation and Coordination of TSA's Secure Flight Program.* OIG-12-94. Retrieved from https://www.oig.dhs.gov/assets/Mgmt/2012/OIGr_12-94_Jul12.pdf

Department of Justice. (n.d.). *The USA patriot act: Preserving life and liberty*. Retrieved from http://www.justice.gov/archive/ll/highlights.htm

Department of the Prime Minister and Cabinet. (2015). Review of Australia's counter-terrorism machinery. Retrieved from https://www.dpmc.gov.au/sites/default/files/publications/190215_CT_Review_0.pdf

Department of the Prime Minister and Cabinet. (2016). National security system. Retrieved from https://www.dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf

Diamond, L. (2007). *Building trust in government by improving governance*. 7th Global Forum on Reinventing Government. Session V: Elections, Parliament, and Citizen Trust. Retrieved from http://stanford.edu/~ldiamond/paperssd/BuildingTrustinGovernmentUNGLobalForum.pdf

Edwards, B. (2015, August 12). Spy agency powers could grow – minister. *Radio New Zealand*. Retrieved from http://www.radionz.co.nz/news/political/281206/spy-agency-powers-could-grow-minister

Engeli, I., & Allison, C. (Eds.). (2014). *Comparative policy studies.* Retrieved from: http://www.pagraveconect.com.proxy.lib.sfu.ca/pc/doifinder/10.1057/9781137314154.0004

Equality and Human Rights Commission. (2012). Article 8: The right to respect for private and family life, home and correspondence. *Human Rights Review*, 259-312. Retrieved from http://www.equalityhumanrights.com/sites/default/files/documents/humanrights/hrr_article_8.pdf

Executive Order 12333, The White House: United States Intelligence Activities, 40 Fed. Reg. 59,941 (Dec. 4, 1981)

Farr, M. (2016, July 25). Turnbull announces tough new laws to combat terrorists. *News*. Retrieved from http://www.news.com.au/national/politics/turnbull-announces-tough-new-laws-to-combat-terrorists/news-story/475412cee06163dd46ade2a8852b59a6

Field, A. (2009). Tracking terrorist networks: Problems of intelligence sharing within the U.K. intelligence community. *Review of International Studies, 35*(4), 997-1009. Retrieved from http://www.jstor.org.proxy.lib.sfu.ca/stable/40588099

Fisher, M. (2016, Feb 17). Lessons on national defence from down under. *National Post.* Retrieved from http://nationalpost.com/opinion/matthew-fisher-lessons-on-national-defence-from-down-under

Flood, P. (2004). *Report of the inquiry into Australian intelligence agencies*. Department of the Prime Minister and Cabinet. Retrieved from http://fas.org/irp/world/australia/flood.pdf

Forcese, C. (2015a). Bill c-51: Catching up on the "catching up with our allies" justifications for new CSIS powers. *National Security Law.* Retrieved from http://craigforcese.squarespace.com/national-security-law-blog/2015/4/16/bill-c-51- catching-up-on-the-catching-up-with-our-allies-jus.html

Forcese, C. (2015b, March 9). *Bill C-51: Do our allies really have similar powers to violate the law?* Retrieved from http://craigforcese.squarespace.com/national-security-law- blog/2015/3/9/bill-c-51-do-our-allies-really-have-similar-powers-to-violat.html

Forcese, C. & Roach, K. (2015a). *Bill c-51 backgrounder #2: The Canadian Security Intelligence Service's proposed power to "reduce" security threats though conduct that may violate the law and the Charter*. Retrieved from: http://www.antiterrorlaw.ca/

Forcese, C. & Roach, K. (2015b). *Proposed amendments to bill c-51, antiterrorism act 2015.* doi 10.2139/ssrn.2576202

Forcese, C. & Roach, K. (2015c). Terrorist babble and the limits of the law: Assessing a prospective Canadian terrorism glorification offence. TSAS Working Paper Series. No. 15-02. Retrieved from: http://library.tsas.ca/media/TSASWP15-02_Forcese-Roach.pdf

Forcese, C. & Roach, K. (2017, June 20). The roses and thorns of Canada's new national security bill. *Macleans.* Retrieved from http://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/

Freese, R. (2014). Evidence-based counterterrorism or flying blind? How to understand and achieve what works. *Perspectives on Terrorism, 8*(1), 37-56.

Golder, B., & Williams, G. (2006) Balancing national security and human rights: Assessing the legal response of common law nations to the threat of terrorism, *Journal of Comparative Policy Analysis: Research and Practice, 8*(1) 43-62, doi: 10.1080/13876980500513335

Greene, R. (2015, April 21). Coalition letter from 55 civil society groups, security experts, academics opposing PSNA. *Open Technology Institute.* Retrieved from http://www.newamerica.org/oti/coalition-letter-from-55-civil-society-groups-security-experts-and-academics-opposing-pcna/

Gregory, F. (2005). Intelligence-led counter-terrorism: A brief analysis of the UK domestic intelligence system's response to 9/11 and the implications of the london bombings of 7 july 2005. *Real Instituto Elcano,* (94), 12. Retrieved from http://www.realinstitutoelcano.org/analisis/781/Gregory781-v.pdf

Guliani, N.S. (2015, June 3). What's next for surveillance reform after the USA Freedom Act. *American Civil Liberties Union.* Retrieved from https://www.aclu.org/blog/washington- markup/whats-next-surveillance-reform-after-usa-freedom-act

Gwyn, C. (2014). *Report into the release of information by the New Zealand security intelligence service in July and August 2011*. Office of the Inspector-General of Intelligence and Security. Public Report. Retrieved from https://s3.amazonaws.com/s3.documentcloud.org/documents/1370356/final-report-into-the-release-of-information-by.pdf

Hall, C. (2017, June 21). National security vs. individual freedoms: How the Liberals aim to strike a balance. *CBC.* Retrieved from http://www.cbc.ca/news/politics/liberal-security-changes-legislation-oversight-analysis-1.4169942

Hall, C. (2015, Feb 20). CSIS watchdog agency starved of staff, resources. *CBC News.* Retrieved from http://www.cbc.ca/news/politics/csis-watchdog-agency-starved-of-staff-resources- 1.2965276

Haugham, J.K. (2016, Nov 16). Combatting terrorism in a digital age: First amendment implications. *NewseumInstitute.* Retrieved from http://www.newseuminstitute.org/first-amendment-center/topics/freedom-of-speech-2/internet-first-amendment/combatting-terrorism-in-a-digital-age-first-amendment-implications/

Hattem, J. (2015, June 2). Obama signs NSA bill, renewing patriot act powers. *The Hill.* Retrieved from http://thehill.com/policy/national-security/243850-obama-signs-nsa-bill-renewing-patriot-act-powers

Holder v. Humanitarian Law Project, 130 S.Ct. 2705 (2010).

Home Office. (2015). *Authority to carry scheme 2015.* Retrieved from

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/41

Home Office. (2014). *Factsheet: border security – aviation, shipping and rail*. Counter-Terrorism and Security Bill: factsheets. Retrieved from https://www.gov.uk/government/collections/counter-terrorism-and-security-bill-factsheets

Home Office. (2012). *The security and travel bans authority to carry scheme*. Retrieved from https://www.gov.uk/government/publications/the-security-and-travel-bans-authority-to- carry-scheme-2012

Hoogensen, G. & Rottem, S. (2004). Gender identity and the subject of security. *Security Dialogue, 35*(2), 155-171. doi 10.1177/0967010604044974.

Human Rights Commission. (2014, November 27). *Countering terrorist fights bill needs amending to better protect human rights*. Retrieved from https://www.hrc.co.nz/news/countering-terrorist-fighters-bill-needs-amending-better-protect-human-rights/

Human Rights Submission Citizenship Bill. (2004, Oct 7). *Scoop Independent News*. Retrieved from http://www.scoop.co.nz/stories/PO0410/S00073/human-rights-f-submission-citizenship-bill.htm

Hunter, M. (2015, April 15). U.S. to tell Americans why they're on no-fly list. *CNN.* Retrieved from http://www.cnn.com/2015/04/15/travel/americans-no-fly-listfeat/9838/49013_Official_ATC_Scheme_accessible.pdf

International Civil Liberties Monitoring Group. (n.d). Bill C-59: Oversight and review mechanisms. Retrieved from http://iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59-oversight-and-review-mechanisms/

James, R. (2015, March 9). “Oral questions – public safety”. Canada. Parliament. Debates of the House of Commons. *Edited Hansard 147*(182). 41st Parliament, 2nd session. Retrieved from http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=7867058&Language= E&Mode=1

Jamshidi, M., & Noori, F. (2017). The United States national security strategy under Bush and Obama: Continuity and change. *Journal of World Sociopolitical Studies, 1*(2), 175-197. Retrieved from https://wsps.ut.ac.ir/article_63616_8235.html

Johnson, J.L, Kartchner, K.M., & Larsen, J.A. (Eds). (2009). Strategic culture and weapons of mass destruction: Culturally based insights into comparative national security policymaking. *Initiatives in strategic studies – issues and policies* (4). London: England: Palgrave Macmillan. Retrieved from https://www.palgrave.com/us/book/9780230612211

Jones, S. (2018, Mar 1). Spanish student has conviction for Twitter joke overturned. The Guardian. Retrieved from https://www.theguardian.com/world/2018/mar/01/spanish-student-cassandra-vera-conviction-twitter-joke-overturned

Joseph, R. & Bronskill, J. (2017, May 19). Majority of Canadians want Bill C-51 repealed: government report. *Global News.* Retrieved from https://globalnews.ca/news/3466160/majority-of-canadians-want-bill-c-51-repealed-government-report/

Karp, P. (2017, Oct 3). Turnbull defends proposed anti-terrorism laws as constitutional. *The Guardian.* Retrieved from https://www.theguardian.com/australia-news/2017/oct/04/turnbull-defends-proposed-anti-terrorism-laws-as-constitutional

Koc-Menard, S. (2006). Australia’s intelligence and passenger assessment programs. *International Journal of Intelligence and Counterintelligence, 19*(218-236). doi: 10.1080/08850600500483681

Konecki, K. (2008). Triangulation and dealing with the realness of qualitative research. *Qualitative Sociology Review, 4*(8), 7-28. Retrieved from http://proxy.lib.sfu.ca/login?url=https://search-proquest-com.proxy.lib.sfu.ca/docview/61722165?accountid=13800

Kopan, T. (2017, Nov 1). Domestic terrorism programs would be cut under Trump. *CNN.* Retrieved from https://www.cnn.com/2017/10/02/politics/trump-administration-cuts-domestic-terrorism/index.html

Krause, K. & Williams, M.C. (1996). Broadening the agenda of security studies: Politics and methods. *Mershon International Studies Review, 40*(2), 229-254. Retrieved from http://www.jstor.org/stable/222776

Lagasse, P. (2015, Feb 26). Should parliament 'oversee' national security affairs? *Centre forInternational Studies*. Retrieved from http://cips.uottawa.ca/should-parliament-oversee-national-security-affairs/

Latif v. Holder, 3:10-cv-00750-BR. United States District Court District of Oregon. Retrieved from https://www.aclu.org/sites/default/files/field_document/latif_revisions_notice.pdf

Liberty. (n.d.-b). *Overview of terrorism legislation.* Retrieved from https://www.liberty-human- rights.org.uk/human-rights/countering-terrorism/overview-terrorism-legislation

Liberty. (n.d.-a). *The People vs The Snoopers' Charter.* Retrieved from https://www.libertyhumanrights.org.uk/campaigning/people-vs-snoopers-charter

Liddicoat, J. (2014). Global information society watch 2014: Communications surveillance in the digital age. 178-181. Retrieved from http://www.giswatch.org/en/country-report/communications-surveillance/new-zealand

Loughrey, C. (2018, Feb 24). Rapper jailed for three and a half years after criticising Spanish royal family. *Independent.* Retrieved from https://www.independent.co.uk/arts-entertainment/music/news/rapper-jailed-lyrics-spanish-royal-family-valtonyc-josep-miquel-arenas-beltran-a8226421.html

Lowe, D. (2014). Surveillance and international terrorism intelligence exchange: Balancing the interests of national security and individual liberty. *Terrorism and Political Violence, 28*(4), 653-673. doi.org/10.1080/09546553.2014.918880

MacAskill, E., Watt, N., & Mason, R. (2015, June 11). UK intelligence agencies should keep mass surveillance powers, report says. *The Guardian.* Retrieved from http://www.theguardian.com/world/2015/jun/11/uk-intelligence-agencies-should-keep-mass-surveillance-powers-report-gchq

MacDonald, N.A. (2011). Parliamentarians and national security in Canada. *Canadian Parliamentary Review, 34*(4), 33-41. Retrieved from http://www.revparl.ca/english/issue.asp?param=208&art=1460

MacLeod, I. (2015, March 18). Spy versus spy: Australian security oversight holds lessons for Canada. *Ottawa Citizen.* Retrieved from http://ottawacitizen.com/news/politics/spy-versus-spy-australian-security-oversight-holds-lessons-for-canada.

Mason, R., & Dodd, V. (2017, June 6). May: I'll rip up human rights laws that impede new terror legislation. *The Guardian.* Retrieved from https://www.theguardian.com/politics/2017/jun/06/theresa-may-rip-up-human-rights-laws-impede-new-terror-legislation

Mayer, A. (Dec 10, 2014). CIA torture report: Why Canada can't claim innocence. *CBC.* Retrieved from http://www.cbc.ca/news/cia-torture-report-why-canada-can-t-claim-innocence-1.2867716

Mazetti, M. & Weisman, J. (2014, March 11). Conflict erupts in public rebuke on C.I.A. inquiry. *The New York Times.* Retrieved from http://www.nytimes.com/2014/03/12/us/cia- accused-of-illegally-searching-computers-used-by-senate-committee.html

McGill, A.K.S. & Gray, D.H. (2012). Challenges to international counterterrorism intelligence sharing. *Global Security Studies, 3*(3). Retrieved from http://globalsecuritystudies.com/McGill%20Intel%20Share.pdf

Minister Blaney speaks to the Canadian Club of Toronto on anti-terrorism measures to better protect Canadians. (2015, Apr 29). *Canada NewsWire*. Retrieved from http://search.proquest.com.proxy.lib.sfu.ca/docview/1676399367?accountid=1380 0

Ministry of Justice. (2013). *Information sharing changes to the Privacy Act 1993.* New Zealand Government. Retrieved from http://www.justice.govt.nz/policy/constitutional-law-and- human-rights/human-rights/domestic-human-rights-protection/privacy-act-1993/privacy-bill

Mohamed v. Holder, 1:11-cv-0050. United States District Court Eastern District of Virginia Alexandria Division. (2015). Retrieved from http://www.fas.org/sgp/jud/gulet/redress.pdf

Moran, J. (2005). State power in the war on terror: A comparative analysis of the UK and USA. *Crime, Law, & Social Change, 44*(4), 335-359. doi:10.1007/s10611-006-9026-4

Nelson, R. (2011, Sept 16). Information sharing in security and counterterrorism. *Centre for Strategic & International Studies.* Retrieved from http://csis.org/publication/information-sharing-security-and-counterterrorism

New Zealand Intelligence Community. (2015a). *About us.* New Zealand Government. Retrieved from http://www.nzic.govt.nz/about-us/

New Zealand Intelligence Community. (2015b). *Oversight.* New Zealand Government. Retrieved from http://www.nzic.govt.nz/oversight/

New Zealand Security Intelligence Service. (n.d.). *Working with other organisations.* New Zealand Government. Retrieved from http://www.nzsis.govt.nz/about-us/working-with- other-organisations/

New CSIS powers not as frightening as they seem: Harper's security advisor. (2015, April 27). *The Canadian Press*. Retrieved from http://www.ctvnews.ca/politics/new-csis-powers-not-as-frightening-as-they-seem-harper-s-security-adviser-1.2347313

New Zealand Law Society. (2015) *Law society urges reduction of terrorist fight bill powers.* Retrieved from https://www.lawsociety.org.nz/news-and-communications/news/2014/november-2014/law-society-urges-reduction-of-terrorist-fighter-bill-powers

New Zealand Ministry of Affairs. (2003). *New Zealand response to the united nations security council counter-terrorism committee*. Security. Retrieved from http://www.mfat.govt.nz/Foreign-Relations/1-Global-Issues/International-Security/0-NZ-UN-Counter-Terrorism-April-04.php

O'Connor, D. R. (2006). *A new review mechanism for the RCMP's national security activities: Commission of inquiry into actions of Canadian officials in relation to maher arar.*

Office of the Director of National Intelligence. (n.d.). *What we do.* Retrieved from: https://www.dni.gov/index.php/what-we-do

Gilmore Print Group. Ottawa, Ontario. Retrieved from http://www.sirc-csars.gc.ca/pdfs/cm_arar_rcmpgrc-eng.pdf

Public Interest Advocacy Centre. (2015). Submission to the Australian law reform commission inquiry *traditional rights and freedoms – encroachments by commonwealth*. Retrieved from http://www.alrc.gov.au/sites/default/files/subs/55._org_public_interest_advocacy_centre_sub.pdf

Office of the Privacy Commissioner of Canada, (2009). *Audit of the passenger protect program transport Canada.* Retrieved from https://www.priv.gc.ca/information/pub/ar-vr/ar- vr_ppp_200910_e.asp#toc4

Office of the Privacy Commissioner of Canada. (2015). *Statement from the privacy commissioner of Canada following the tabling of bill c-51.* Retrieved from https://www.priv.gc.ca/media/nr-c/2015/s-d_150130_e.asp

Parliamentary Office of Science & Technology. (2014). Big data, crime and security. Houses of Parliament. 1-5. Retrieved from http://www.parliament.uk/post

Price, M. (2013). *National security and local police*. Brennan Center For Justice. New York University School of Law. Retrieved from https://www.brennancenter.org/sites/default/files/publications/NationalSecurity_LocalPol ice_web.pdf

Public Safety Canada. (2017, May 19). National security consultations: What we learned report. *Government of Canada.* Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx

Public Safety Canada. (2016). Our security, our rights: national security green paper 2016. *Background Document.* Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx

Public Safety Canada. (2015a). *Amending the canadian security intelligence service act to give CSIS the mandate to intervene to disrupt terror plots while they are in the planning stages*. Backgrounder. Retrieved from http://news.gc.ca/web/article-en.do?nid=926869

Public Safety Canada. (2014). *Feature focus 2014: Responding to violent extremism and travel abroad for terrorism-related purposes.* Retrieved from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/index-

Public Safety Canada, (2015b). *Passenger protect program*. Backgrounder. Retrieved from http://news.gc.ca/web/article-en.do?nid=926839

Public Safety Canada (2015). *Security of Canada Information Sharing Act: Public Framework.* Government of Canada. Retrieved from http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/shrng-frmwrk-eng.aspx

Prime Minister of Australia. (2017, June 13). National security statement. *Defence and National Security.* Retrieved from https://www.pm.gov.au/media/national-security-statement

Privacy Commissioner. (2014). *Countering terrorist fighters legislation bill.* Retrieved from https://www.privacy.org.nz/assets/Files/Reports-to-ParlGovt/2014-11-27-Select-committee-submission.pdf

Reilly, T. P. (2004). The National Security Strategy of the United States: Development of Grand Strategy. *U.S. Army War College Strategy Research Project*, Carlisle, PA, 14. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a424247.pdf

Risen, T. (2015a, April 22). House approves controversial cybersecurity bill. *U.S. News.* Retrieved from http://www.usnews.com/news/articles/2015/04/22/house-approves-controvesial-cybersecurity-bill

Risen, T. (2015b, March 3). Privacy criticism precedes senate cybersecurity bill. *U.S. News.* Retrieved from http://www.usnews.com/news/articles/2015/03/03/privacy-criticism-precedes-senate-cybersecurity-bill

Rix, M. (2006) Australia's anti-terrorism legislation: the national security state and the community legal sector. *University of Wollongong.* Retrieved from http://ro.uow.edu.au/cgi/viewcontent.cgi?article=1003&context=gsbpapers

Roach, K. (2012). Counter-terrorism in and outside Canada and in and outside the anti-terrorism act. *Review of Constitutional Studies, 16*(2), 243-264. Retrieved from http://web.a.ebscohost.com.proxy.lib.sfu.ca/ehost/pdfviewer/pdfviewer?sid=8401578f- f8db-4834-ab01-410278217e57%40sessionmgr4005&vid=1&hid=4106

Roach, K. (2011). *The 9/11 effect: Comparative counter-terrorism*. New York: Cambridge University Press.

Roach, K., & Forcese, C. (2015a). *Bill c-51 backgrounder #3: Sharing information and lost lessons from the maher arar experience.* http://dx.doi.org/10.2139/ssrn.2565886

Roach, K., & Forcese, C. (2015b). *Bill c-51 backgrounder #1: The new advocating or promoting terrorism offence*. Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2560006

Robertson, D. (2014, October 14). CSIS getting more powers to track suspected terrorists as details emerge of new federal anti-terror bill. *National Post.* Retrieved from http://news.nationalpost.com/news/canada/canadian-politics/csis-to-get-more-powers-to-track-suspected-terrorists-as-details-emerge-of-new-federal-bill

Rosenbach, E. & Peritz, A. (2009). *Confrontation or collaboration? Congress and the intelligence community*. Belfer Center for Science and International Affairs, Harvard Kennedy School. Retrieved from http://belfercenter.ksg.harvard.edu/files/IC-book- finalasof12JUNE.pdf

Ruby, C., & Hasan, N.R. (2015). Bill c-51: A legal primer. *Overly broad and unnecessary anti-terrorism reforms could criminal free speech*. Retrieved from https://www.policyalternatives.ca/publications/monitor/bill-c-51-legal-primer

Ryerson, S., Hiebert, D., & Brooks, L. (2017). On the creation of the office of the community outreach and counter-radicalization coordinator. *Terrorism, Security, and Society.* Retrieved from http://tsas.ca/policy-brief-on-the-creation-of-the-office-of-the-community-outreach-and-counter-radicalization-coordinator/

Sales, N.A. (2010a). Mending walls: Information sharing after the USA patriot act. *Texas Law Review, 88*(7), 1795-1854. Retrieved from http://web.b.ebschost.com/ehost/pdfviewer/pdfviewer?sid=94f14539-8465-454d-85a93c8240816242%40sessionmgr113&vid=2&hid=116

Sales, N.A. (2010b). Share and share alike: Intelligence agencies and information sharing. *George Washington Review, 78*(2), 279-352. Retrieved from http://heinonline.org/HOL/Index?index=journals/gwlr&collection=journals

Sallot, J. (2009, April 6). How Canada failed citizen maher arar. *The Globe and Mail.* Retrieved from http://www.theglobeandmail.com/news/national/how-canada-failed-citizen-maher-arar/article1103562/?page=all

Sample, M.S. (2008). Canada's anti-terrorism act: creating a paradigm of insecurity. Dissertation. Retrieved from SFU Summit.

Secret Intelligence Service. (2015). "About us." Retrieved from https://www.sis.gov.uk/about- us.html

Security Intelligence Review Committee. (2015). Frequently asked questions. Retrieved from http://www.sirc-csars.gc.ca/faqfqs/index-eng.html

Security Intelligence Service. (n.d.-a) “About us.” New Zealand Government. Retrieved from http://www.nzsis.govt.nz/about-us/

Security Intelligence Service. (n.d.-b) “Oversight.” New Zealand Government. Retrieved from http://www.nzsis.govt.nz/about-us/

Security Service. “How we work.” U.K. Government. Retrieved from https://www.mi5.gov.uk/home/about-us/how-we-operate.html

Security Service. (2015). Joint terrorism analysis centre. Retrieved from https://www.mi5.gov.uk/home/about-us/who-we-are/staff-and-management/joint-

Sinai, J. (2015, January 26). The new terrorist threats against Canada & the components of effective countermeasures. The Mackenzie Institute. Retrieved from http://www.mackenzieinstitute.com/new-terrorist-threats-canada-components-effective-countermeasures/

Smith, J. E. (2003). *New Zealand’s anti-terrorism campaign: Balancing civil liberties, national security, and international responsibilities*. Fullbright, New Zealand. Retrieved from http://www.fulbright.org.nz/publications/2003-smith/terrorism-analysis-centre.html

Spy laws passed in senate: ASIO given new powers. (2014, Sept 26). *News Network.* Retrieved from http://www.news.com.au/technology/online/spy-laws-passed-in-senate-asio-given-new-powers/story-fnjwmwrh-1227071116071

Stewart, B. (Oct 28, 2014). Don’t overload CSIS: The case for a separate foreign spy agency. *CBC.* Retrieved from https://www.cbc.ca/news/politics/don-t-overload-csis-the-case-for-a-separate-foreign-spy-agency-1.2814885

Stolberg, A.G. (2012). How nation-states craft national security strategy documents. Strategic Studies Institute. Retrieved from http://publications.armywarcollege.edu/pubs/2201.pdf

Tadjeh, Y. (2015). Big data helping to pinpoint terrorist activities, attacks. *National Defense.* Retrieved from http://www.nationaldefensemagazine.org/archive/2015/April/Pages/BigDataHelpingtoPinpointTerroristActivitiesAttacks.aspx

Tembo, E. B. (2014). *US-UK counter-terrorism after 9/11: A qualitative approach.* Routledge, New York: New York. Retrieved from http://lib.myilibrary.com.proxy.lib.sfu.ca/ProductDetail.aspx?id=563224

Terrorism Act 2006, 2006 c.11, s. 1.

Terrorism act 2006. (2009, Jan 19). *The Guardian*. Retrieved from http://www.theguardian.com/commentisfree/libertycentral/2009/jan/19/terrorism-act-2006

The Associated Press. (Nov 20, 2017). ICC seeks to investigate CIA, U.S. military for alleged war crimes. *CBC.* Retrieved from http://www.cbc.ca/news/world/icc-investigation-afghanistan-cia-haqqani-1.4410463

The Canadian Press. (2017, June 20). Security bill limits CSIS disruption powers, boosts review of spy services. *National Post.* Retrieved from http://nationalpost.com/pmn/news-pmn/canada-news-pmn/newsalert-bill-creates-new-super-watchdog-to-oversee-intelligence-agencies

The National Council for Civil Liberties. 2014. Liberty's second reading briefing on the counter-terrorism and security bill in the house of commons. Retrieved from https://www.liberty-human-rights.org.uk/sites/default/files/Liberty's Second Reading Briefing on the Counter-Terrorism %26 Security Bill in the House of Commons.pdf

The Report of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar. *Report of the events relating to maher arar: Analysis and recommendations.* Public Works and Government Services Canada, Ottawa: Ontario. Retrieved from http://www.sirc-csars.gc.ca/pdfs/cm_arar_rec-eng.pdf

The U.S. moves forward on its no-fly list, Canada moves back. (2015, April 28). *The Globe and Mail.* Retrieved from http://www.theglobeandmail.com/globe-debate/editorials/the-us-moves-forward-on-its-no-fly-list-canada-moves-back/article24157553/

Transportation Security Administration. (n.d.). Security screening. *Department of Homeland Security.* Retrieved from http://www.tsa.gov/travel/security-screening

Tunney, C. (2018a, Feb 28). Families celebrating $81m in budget to fix the no-fly list system. *CBC.* Retrieved from http://www.cbc.ca/news/politics/no-fly-list-families-1.4543329

Tunney, C. (2018b, Jun 20). Some of CSIS's practices still fall outside law: spy watchdog. *CBC.* Retrieved from https://www.cbc.ca/news/politics/csis-report-sirc-information-sharing-1.4714161)

Tunney, C. (2016, Sept 8). Liberals identify 10 key national security issues for public consultations. *CBC.* Retrieved from http://www.cbc.ca/news/politics/ralph-goodale-national-security-public-1.3753329

U.K. Government. *Foreign travel advice: USA.* Retrieved from https://www.gov.uk/foreign travel-advice/usa/terrorism

United Nations, *United Nations Action to Counter-Terrorism*, (17 August, 2015). Retrieved from http://www.un.org/en/terrorism/strategy-counter-terrorism.shtml

United Nations Security Council. (2005, Sept 14). *Prohibition of incitement to commit terrorist acts,* S/RES/1624. Retrieved from http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N05/510/52/PDF/N0551052.pdf?OpenElement

United States. (2017). The national security strategy of the United States of America. Washington: President of the U.S.

USA Freedom Act of 2015. H.R. 2048 (2015). Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/2048/text

Vale, P. (2016, Feb 17). British home secretary Theresa May tells five eyes security group extremists are exploiting migration. *Huffington Post.* Retrieved from http://www.huffingtonpost.co.uk/2016/02/16/theresa-may-extremists-mass-migration_n_9248678.html

Vance, A. (2015). NZ spies want greater powers*. Stuff*. Retrieved from http://www.stuff.co.nz/national/politics/71090362/nz-spies-want-greater-powers

Vicinanzo, A. (2015, March 3). Gaps in info sharing continue to hinder counterterrorism efforts. *Homeland Security Today.* Retrieved from http://www.hstoday.us/briefings/daily-news- analysis/single-article/gaps-in-info-sharing-continue-to-hinder-counterterrorism-efforts/b365f132d73fa2a44e1966dfbee3340a.html

Walker, C. (2014, April 1). *The terrorism suppression act and criminalization of national liberation groups*. Human Rights Blog. Retrieved from http://nzhumanrightsblog.com/uncategorized/the-terrorism-suppression-act-and-criminalisation-of-national-liberation-groups/

Warshawsky, M. (2013). The balance to be found between civil liberties and national security. *The RUSI Jounrnal, 158*(2), 94-99. doi.org/10.1080/03071847.2013.787753

Watters, H. (2015, May 25). Bill C-51: 'No prosperity without security,' steven blaney says. CBC News. Retrieved from http://www.cbc.ca/m/touch/news/story/1.3086424

Weller, G. R. (2001). Change and development in the New Zealand security and intelligence services. *The Journal of Conflict Studies, 21*(1). Retrieved from https://journals.lib.unb.ca/index.php/jcs/article/view/4290/4882

Wilson, D., & Weber, L. (2008). Surveillance, risk and preemption on the Australian border. *Surveillance & Society*, 5(2), 124-141. Retrieved from http://www.surveillance-and-society.org/articles5(2)/australia.pdf

With c-51's new powers, is CSIS simply catching up to allies? (2015, July 16). *CBC News*. Retrieved from http://www.cbc.ca/m/news/politics/with-c-51-s-new-powers-is-csis- simply-catching-up-to-allies-1.3154490

Young, A. (2014, Nov 26). New legislation to allow SIS surveillance may not get enough support. *New Zealand Herald*. Retrieved from http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11364852

18 *U.S.C*. s. 2339A