

LINCOLN MEMORIAL UNIVERSITY LAW REVIEW

VOLUME 3 FALL 2015

COWARDLY TRAITOR OR HEROIC WHISTLEBLOWER?: THE IMPACT OF EDWARD SNOWDEN'S DISCLOSURES ON CANADA AND THE UNITED KINGDOM'S SECURITY ESTABLISHMENTS

*Daniel Alati*¹

The 'world's most wanted man,' Edward Snowden, might be one of the most polarizing figures in modern history. This is particularly true in the United States, where the debates pertaining to his leaks of classified information could not be more divided. Many Americans, including senior level government officials, have publicly argued that Snowden is a cowardly traitor, and have forcefully stated their belief that Snowden should return home to face a myriad of criminal charges, including those under the 1917 Espionage Act. However, many others have gone to great lengths and taken immense personal risks to support Snowden and help further his goal of bringing to light some of the most egregious surveillance abuses ever released into the public sphere.

¹ Dr. Daniel Alati is a post-doctoral researcher at the City University of Hong Kong. His doctoral studies at the University of Oxford focused on comparative anti-terrorism mechanisms in Canada and the United Kingdom.

Snowden's closest confidants are still eager to tell his story: Laura Poitras' documentary 'Citizenfour' has received rave reviews² and long-time NSA critic and journalist James Bamford recently interviewed Snowden in Moscow for WIRED magazine.³ They continue to release leaked documents that expose the greatest abuses of the global surveillance machine Glenn Greenwald's website, *The Intercept*, reported recently that Canada's leading surveillance agency is analyzing records of up to fifteen million downloads daily to track extremists.⁴ As a result, it seems likely that the Snowden leaks, already considered by many to be the most infamous example of whistleblowing of all time, will be a topic of American and global conversation for years to come.

However, what is less clear is what kind of tangible legislative change (if any) the Snowden leaks will bring about, particularly in countries other than the U.S. While much has been written about how the Snowden leaks have, and will continue to, influence American domestic policy and American diplomatic and intelligence-sharing arrangements with other nations, less has been written about the impact that the leaks have had on some of the U.S.' most important allies. This paper analyzes what impact the Snowden leaks have had in Canada and the United Kingdom. Sections one and two analyze the impact the Snowden disclosures have had on civil society. In doing so, it notes a glaring lack of parliamentary mechanisms for oversight of intelligence activities in Canada and also illuminates issues with the existing mechanisms in the UK. Section three examines what, if any, tangible legislative outcomes have resulted from the Snowden leaks. It concludes that it is difficult to assign any tangible legislative

² Peter Bradshaw, *Citizenfour Review – Gripping Snowden Documentary Offers Portrait of Power, Paranoia, and One Remarkable Man*, THE GUARDIAN, Oct. 16, 2014,

<http://www.theguardian.com/film/2014/oct/16/citizen-four-review-edward-snowden-documentary>.

³ James Bamford, *Edward Snowden: The Untold Story*, WIRED MAG., Aug. 22, 2014, <http://www.wired.com/2014/08/edward-snowden/>.

⁴ Ryan Gallagher & Glenn Greenwald, *Canada Casts Global Surveillance Dragnet Over File Downloads*, THE INTERCEPT, Jan. 28, 2015, <https://firstlook.org/theintercept/2015/01/28/canada-cse-levitation-mass-surveillance/>.

outcomes in either country to the leaks. Finally, in the concluding section, recommendations for changes to the oversight mechanisms in both countries that may help to prevent the reoccurrence of some of the most egregious abuses exposed by the Snowden leaks are posited.

I. CANADA – IMPACT OF SNOWDEN DISCLOSURES ON CIVIL SOCIETY

Unsurprisingly, in the aftermath of the Snowden disclosures there was a significant amount of material published by Canadian academics, legal associations, judges, standing committee members, Parliamentarians and the media. This was to be expected as “Snowden’s revelations have implicated Canada’s foreign intelligence signals agency – the *Communications Security Establishment Canada* (CSEC) – in expansive domestic and foreign surveillance initiatives.”⁵ Some of these expansive and troubling initiatives, which implicated both CSEC and other Canadian officials, include: CSEC using airport Wi-Fi to track Canadian travelers;⁶ CSEC setting up hidden spying posts in about twenty countries in which it conducted espionage at the behest of the NSA;⁷ Canada allowing the NSA to spy on Canadian soil during the 2010 G8 and G20 Summits;⁸ Canadian embassies overseas

⁵ Simon Davies, *A Crisis of Accountability: A Global Analysis of the Impact of the Snowden Revelations*, THE PRIVACY SURGEON 22 (2014), <https://citizenlab.org/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf>.

⁶ Greg Weston, Glenn Greenwald & Ryan Gallagher, *CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden documents*, CBC NEWS, Jan. 30, 2014, <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>.

⁷ Greg Weston, Glenn Greenwald & Ryan Gallagher, *Snowden Document Shows Canada Set Up Posts for NSA*, CBC NEWS, Dec. 9, 2013, <http://www.cbc.ca/news/politics/snowden-document-shows-canada-set-up-spy-posts-for-nsa-1.2456886>.

⁸ Greg Weston, Glenn Greenwald & Ryan Gallagher, *New Snowden Docs Show U.S. Spied During G20 in Toronto*, CBC NEWS, Nov. 27, 2013, <http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448>.

using eavesdropping technology;⁹ and, finally, allegations that Canadian spies collected metadata of phone calls and e-mails to and from Brazil's Mines and Energy Ministry.¹⁰ While these are only some examples of deeply worrisome Canadian complicity in NSA activity, they underscore one of the most significant areas of concern to be expressed by Canadian civil society: the deep inter-connection between Canada and the United States and the corresponding connection between their intelligence activities. That Canada and the U.S. share deep economic, geographic, and cultural ties is no secret, but the extreme inter-connectedness of these two countries (and its impact on their intelligence-sharing relationships) begs further elucidation.

Farson and Teeple note that, "[t]he significance of the long-standing economic relationship with the U.S. may be even greater today for both parties, particularly given that other traditional political and military allies are now economic competitors. Certainly, it has become ever more integrated with both countries remaining each other's most significant trading partner."¹¹ Moreover, Farson and Teeple point to many other shared linkages between the countries that are crucial to their intelligence sharing relationships, namely, critical telecommunications and security infrastructure, and argue that Canada has been seen as a "freeloader" because of the imbalance between the two countries' differing contributions to North American defence and security.¹² Canada, like the UK, is a member of the "Five Eyes" community that

⁹ Colin Freeze, *Canadian Embassies Eavesdrop, Leak Says*, THE GLOBE & MAIL, Oct. 29, 2013, <http://www.theglobeandmail.com/news/world/canada-involved-in-us-spying-efforts-abroad-leaked-document-says/article15133508/>.

¹⁰ *Canadian Spies Targeted Brazil's Mines Ministry: Report*, CBC NEWS (Oct. 7, 2013), <http://www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975>.

¹¹ Stuart Farson & Nancy Teeple, *Increasing Canada's Foreign Intelligence Capability: Is it a Dead Issue?*, INTELLIGENCE & NAT'L SECURITY, Vol. 30, 47, 59 (2015).

¹² *Id.* at 60.

pools their resources, divide targets according to geographic location and expertise, and share analyses. In all cases, the NSA is the big brother. In some instances, it helps fund the activities of its partners in order to influence intelligence gathering programs. . . . Canada's contribution focuses on the northern regions of Russia and China, Latin America, as well the northern parts of the Atlantic and Pacific Oceans.¹³

Academic commentators have criticized various aspects of the intelligence sharing relationships between the two countries. Clement has noted that,

[w]ell before the Snowden revelations, CIRA commissioned an expert study of the Canadian Internet infrastructure, which compared all Canadian routings with those that transited the United States and found significant inefficiencies with the boomerang routing. CIRA's report concluded that Canadian Internet access is heavily and unnecessarily dependent upon foreign infrastructure, especially US infrastructure.¹⁴

He laments the fact that much of Canada's internal Internet traffic is routed through the US, noting that the lack of international submarine fiber optic cables in Canada means that "almost all of Canada's third country Internet traffic is similarly routed through the United States and via NSA surveillance operations."¹⁵ While some Canadian Internet companies, such as Bell Canada, have seized upon this opportunity to offer "safer, more private, domestic" Internet

¹³ *Id.* at 63.

¹⁴ Andrew Clement, *Canada's Bad Dream*, *WORLD POL'Y J.*, Vol. 31, 25-33, 30 (2014), available at <http://www.worldpolicy.org/journal/fall2014/canada's-bad-dream>.

¹⁵ *Id.* at 27.

solutions,¹⁶ the post-Snowden climate in Canada still represents what Wesley Wark calls a “hopeful and distressing reality.”¹⁷ According to Wark, it is

[h]opeful in the sense that we can anticipate a kind of recalibration of US-led global surveillance which might accord with our own principles and interests; distressing in that it reveals that Canada, enmeshed in its dependency on the NSA, and suffering problems of endemic secrecy, inadequate laws, poor accountability, hands-off political leadership, and an ill-informed public, cannot make independent headway in coming up with our own, applied Snowden verdict on global surveillance.¹⁸

Other than the issues noted above, there are several obstacles to the effective development and operation of a specifically Canadian system of intelligence oversight and accountability. The first is cultural. As Jeffrey Roy notes,

[t]here is often a tendency in Canada to view such activity with a certain detachment and smugness: thank goodness that’s not us. Yet, almost every significant scandal involving government action in the US has been accompanied by revelations in Canada that public sector authorities are acting in a remarkably similar manner.¹⁹

The second, more significant obstacle, is the lack of any established parliamentary review mechanisms that provide for

¹⁶ *Id.* at 27-28.

¹⁷ Loch K. Johnson et. al, *An INS Special Forum: Implications of the Snowden Leaks*, INTELLIGENCE & NAT’L SECURITY, Vol. 29, 793-810 (2014).

¹⁸ *Id.*

¹⁹ Jeffrey Roy, *Secrecy, Security and Digital Literacy in an Era of Meta-Data: Why the Canadian Westminster Model Falls Short*, INTELLIGENCE & NAT’L SECURITY, 2-3 (2015).

any kind of meaningful oversight or accountability. As will be discussed further below, attempts to set up a National Security Committee of Parliamentarians have been stymied for over a decade, despite support for such a Committee stemming from judicial inquiries, reports of parliamentary committees, civil society organizations and the wider legal community. The result is the “absence of such oversight altogether, which is how one can reasonable characterize the Canadian model. With the partial exception of Ministers directing them, Canadian Parliamentarians are shielded from scrutinizing security authorities in any direct and meaningful manner.”²⁰

In order to more fully understand Canada’s current lack of meaningful mechanisms for parliamentary review and accountability of intelligence service activities, several stymied attempts on behalf of Canadian civil society actors over the course of the last decade must be noted. The first unsuccessful attempt to create a novel Parliamentary Committee on National Security (composed of both MPs and Senators from across party lines) occurred in 2005 under a Liberal minority government with the tabling of Bill C-81.²¹ Despite cross-party support, that bill died on the order paper following the 2005 dissolution of the Canadian Parliament. The continuing lack of effective parliamentary oversight was subsequently criticized by two separate, independent judicial reviews carried out by Justices O’Connor and Iacobucci pertaining to the actions of Canadian officials in the war on terror (in particular, CSIS and the RCMP).²² In particular, O’Connor noted that the rendition experienced by Maher Arar urgently emphasized that Canada was in need of an independent national security review framework. A Standing Committee on Public Safety and National Security tasked with reviewing Iacobucci and O’Connor’s findings and recommendations would later in 2009 find it “regrettable that the government

²⁰ *Id.* at 7.

²¹ Full text, legislative history, and additional information pertaining to the bill *available at* <http://openparliament.ca/bills/38-1/C-81/>.

²² Government of Canada Publications, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin*, http://publications.gc.ca/collections/collection_2010/bcp-pco/CP32-90-1-2010-eng.pdf.

has not yet established the independent national security review framework recommended by Justice O'Connor" and argue that said framework was "essential to prevent further human rights violations."²³ They forcefully added that "there was an urgent need for action" and that without an integrated structure for the full review of national security issues, Canadians would be at further risk of violations of their rights and freedoms.²⁴

To this date, no mechanism for parliamentary oversight of intelligence or security mechanisms in Canada, along the lines of that proposed in Bill C-81 or envisioned by Justice O'Connor, exists.²⁵ The ignorance of this alarming lack of oversight seems to be a trend continuing through successive Canadian governments that now continues under the current Conservative government's administration. For example, as noted by Roy,

[a] report published by the federal Privacy Commissioner in early 2014, in line with much of the earlier analysis of the Canadian apparatus, calls for fundamental political reforms too ineffective or simply absent mechanisms for overseeing the data gathering activities of Canadian federal authorities as well as the public and private sectors more widely.

²³ Ottawa Standing Committee on Public Safety and National Security, *Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries*, <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=4004074>.

²⁴ *Id.* at 11-17. Recommendation five of this report states that, "[t]he Committee recommends, once again, that Bill C-81, introduced in the 38th Parliament, An Act to Establish the National Security Committee of Parliamentarians, or a variation of it, be introduced in Parliament at the earliest opportunity."

²⁵ Two Bills (S-220, *infra* note 32, and C-551, *infra* note 33) have been introduced in both the House and the Senate that continue the work of Bill C-81, although neither bill has made any kind of significant progress. For example, Bill C-551 was introduced into the House in November of 2013 and has yet to progress, while Bill S-220 was introduced into the Senate in May 2014 and has still yet to pass Second Reading. *Id.*

The report was widely applauded by Canadian security experts, though largely ignored by the Government itself.²⁶

It is within this context of ignorance that the concerns of Canadian civil society echo even louder. The *Protect Our Privacy Coalition*, which is made up of more than fifty civil society organisations, has launched an online initiative calling on Members of Parliament to introduce restrictions that would curtail CSEC's most egregious abuses.²⁷ Moreover, the British Columbia Civil Liberties Association is constitutionally challenging aspects of CSEC's legal and operational framework,²⁸ and the Canadian Civil Liberties Association has also launched a lawsuit challenging the constitutionality of PIPEDA, Canada's federal data protection statute.²⁹ Moreover, the Privacy Commissioner has released a statement regarding telecommunications companies' responses to information requests from government authorities, in which a number of recommendations are made, particularly in regards to the transparency of authorized disclosures.³⁰

In addition to these civil society actors, a number of interested Members of Canadian Parliament have tried to push for additional debate pertaining to CSEC's activities and Canada's glaring lack of parliamentary overview of

²⁶ Roy, *supra* note 19 at 17-18.

²⁷ See OPEN MEDIA, <https://openmedia.ca/ourprivacy> (last visited Oct. 23, 2015).

²⁸ The litigation is ongoing. See Globe Editorial, *Hey CSEC, Stop Spying on Me*, THE GLOBE & MAIL, Apr. 2, 2014, <http://www.theglobeandmail.com/globe-debate/editorials/dont-spy-on-me-csec/article17781948>.

²⁹ The litigation is ongoing. See Alex Boutilier, *Canadian Civil Liberties Group Launches Court Challenge on Warrantless Access*, THE TORONTO STAR, May 21, 2014, http://www.thestar.com/news/canada/2014/05/21/canadian_civil_liberties_group_launches_court_challenge_on_warrantless_access.html.

³⁰ See Office of the Privacy Commissioner of Canada, *Statement from the Interim Privacy Commissioner of Canada Regarding Telecommunications Companies' Responses to Information Requests from Government Authorities*, https://www.priv.gc.ca/media/nr-c/2014/s-d_140430_e.asp.

intelligence activities. In calling for an emergency debate on CSEC's meta-data collection program, MP Charmaine Borg argued that,

[a]n emergency debate is needed so that parliamentarians can take an in-depth look at the extent to which Canadians' personal information, metadata and other information are collected by the police, law enforcement agencies and national security agencies. This debate is also needed so that we can look at measures that will lead to appropriate parliamentary oversight and ways to balance public and national security interests with Canadians' privacy rights.³¹

Moreover, as aforementioned, interested members of Parliament have introduced two bills (S-220³² and C-551³³) in order to further the work of C-81 and create a Parliamentary Committee for the oversight of national security and intelligence activities. The current Canadian government's response (or lack thereof) to the various efforts of academics and other civil society actors outlined in this section will be considered in this paper's subsequent analysis of tangible legislative outcomes to result from the Snowden disclosures.

II. UNITED KINGDOM – IMPACT OF SNOWDEN DISCLOSURES ON CIVIL SOCIETY

³¹ *Charmaine Borg on Request for Emergency Debate*, June 13, 2013, <http://openparliament.ca/debates/2013/6/13/charmaine-borg-1/only/>.

³² An Act to Establish the Intelligence and Security Committee of Parliament, <http://www.parl.gc.ca/legisinfo/BillDetails.aspx?billId=6556209&Language=E&Mode=1>

³³ National Security Committee of Parliamentarians Act, <http://www.parl.gc.ca/legisinfo/BillDetails.aspx?billId=6256801&Language=E&Mode=1>.

Whereas the Snowden disclosures in Canada and the United States sparked widespread civil society debate and condemnation, reaction to the disclosures in the United Kingdom has been markedly different, particularly in regards to the responses from the political classes. As Martin Moore notes,

[t]he reaction in the UK has to date been startlingly different. The political class jointly defended the actions of the security services, and most shied away from proposing reform of the law. The press was split on their response, some recommending prosecution of the messenger, *The Guardian*. . . . It is difficult to explain why the reaction in the two countries has been so different. No doubt partly it is cultural, and partly due to contrasting public attitudes in the UK and US to the role of the state. It must also be due in part to the UK's intelligence services' importance to its international status. Intelligence remains one area where the UK is considered, in terms of expertise and performance, to be on a par with global superpowers.³⁴

As was the case with CSEC in Canada, the material disclosed by Snowden implicated the UK's counterpart GCHQ (Government Communications Head Quarters) in various spying activities. Mark Young notes that, "British government concerns about the potential publication of classified data were significant enough to threaten *The Guardian* with legal action if the information was not destroyed. The threats prompted the destruction of hard drives containing information related to GCHQ."³⁵

³⁴ Martin Moore, *RIP RIPA? Snowden, Surveillance, and the Inadequacies of our Existing Legal Framework*, THE POL. Q., Vol. 85, No. 2, 125-132, 125-126 (2014).

³⁵ Mark Young, *National Insecurity: The Impacts of Illegal Disclosures of Classified Information*, I/S: A J. OF LAW & POL'Y FOR THE INFO. SOC'Y, Vol. 10, 367, 368 (2014).

The United Kingdom has been placed in a particularly precarious position by the Snowden disclosures because of its relationship with the European Union. As was the case with Canada and the United States, the United Kingdom and the European Union share a vast inter-connectedness in several fields, including intelligence sharing and gathering. For instance, Bauman notes that, “[t]he UK has been in an especially delicate position given that GCHQ has participated in aggressive behavior against other partners and EU institutions while being part of the European Union and having signed the EU treaty which requires member states’ loyalty.”³⁶ Again, similar to what was the case in Canada and the United States, much of Europe’s Internet traffic is routed through the United Kingdom. As Brown and Korff note, the UK

is the landing point for the majority of transatlantic fibre-optic cables. GCHQ has reportedly placed data interceptors on fibre-optic cables conveying internet data in and out of the UK, and are able to store a significant fraction of global Internet traffic for three days on a rolling basis while carrying out further automated analysis.³⁷

Despite Canada’s connections to the United States, and the UK’s connection to Europe, it is clear that the NSA and the GCHQ have invested more resources in their activities than any other organisations on earth. As Bauman notes,

[t]he NSA has a budget of US \$10.8 bn (7.8 bn Euros) a year, whereas within Europe GCHQ’s budget of 1.2 bn Euros is well below the NSA, but nevertheless over twice the yearly budget of other agencies such as BND, FRA, or DGSE. This is why it may be more accurate to speak of

³⁶ Zygmunt Bauman et. al, *After Snowden: Rethinking the Impact of Surveillance*, INT’L POL. SOC., Vol. 8, 121-144, 127 (2014).

³⁷ Ian Brown & Douwe Korff, *Foreign Surveillance: Law and Practice in a Global Digital Environment*, EUROPEAN HUM. RTS L. REV., Vol. 3, 243-251, 243 (2014).

an Anglo-American guild of professionals extended to other Western intelligence services than to analyze the network as a US-European collaboration on an equal footing, or even a transatlantic collaboration correlated with NATO.³⁸

Unlike Canada, the United Kingdom does have various mechanisms for oversight of national security and intelligence activities, which has led to a variety of pre and post-Snowden analyses and recommendations for change. As Sudha Setty notes,

[n]umerous parliamentary committees have undertaken investigations of the surveillance apparatus in the United Kingdom. A broad investigation by the Constitution Committee led to findings in 2009 that the intelligence-gathering services were largely compliant with the law, but that report included numerous recommendations for changes to surveillance authority and transparency, including giving greater consideration to civil liberties before implementing further surveillance programs, granting greater authority to various commissioners to exercise increased oversight, revisiting existing legislation to increase specificity in the surveillance authority, and making the work of the Investigatory Powers Tribunal more transparent.³⁹

Writing in Martin Moore's piece, Jenna Stratford, QC agrees that there are flaws with the Investigatory Powers Tribunal, namely that "[w]here complaints are rejected, as the huge majority unsurprisingly are, claimants are not given proper reasons but instead the judicial equivalent of a 'neither confirm nor deny' notice. In addition, at present there is no possibility of appeal from the Tribunal's decisions, so that

³⁸ Bauman, *supra* note 36.

³⁹ Sudha Setty, *Surveillance, Secrecy, and the Search for Meaningful Accountability*, 51 STAN. J. INT'L L. 69 (2015).

probably the only recourse is to Strasbourg.”⁴⁰ Furthermore, the Intelligence and Security Committee considered whether GCHQ’s receipt of information by the NSA from the PRISM program was legal, ultimately finding that the GCHQ’s actions were compliant with the statutory framework, but concluding that the framework required additional specificity.⁴¹

A further complication arises in the United Kingdom because of the operation of the Regulation of Investigatory Powers Act (RIPA).⁴² As Setty notes, under the operation of this act,

[t]he sole recourse for challenging such actions under U.K. law is making a claim to the Investigatory Powers Tribunal and that, although the Human Rights Act 1998 incorporates the European Convention on Human Rights (“ECHR”) into U.K. domestic law, if the judiciary believes that a national security measure is incompatible with the ECHR standard, it may declare incompatibility but this does not constitute a mandate that the domestic security apparatus change its policies. As such, review at the domestic level has often been sharply curtailed.⁴³

RIPA has been criticized by many as an outdated piece of legislation that does not fit the current realities of our technologically advanced world. Lord Ken Macdonald QC, who was the Director of Public Prosecutions in England and Wales from 2003-2008, argues that RIPA “was not written in the age of social media and big data. It is inherently

⁴⁰ Moore, *supra* note 34.

⁴¹ Intelligence and Security Committee of Parliament, *Statement on GCHQ’s Alleged Interception of Communications under the US PRISM Programme*, July 17, 2013, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/225459/ISC-Statement-on-GCHQ.pdf.

⁴² Regulation of Investigatory Powers Act 2000, <http://www.legislation.gov.uk/ukpga/2000/23/contents>.

⁴³ Setty, *supra* note 39.

backwardlooking” and Jenna Straford echoes this sentiment by stating that, “RIPA contains only limited restrictions on the transfer of data to third-party powers. The Secretary of State has extremely wide discretion—almost unfettered in practice—to determine whether data may be transferred.”⁴⁴

Despite the aforementioned varying responses by the media and political classes following the Snowden revelations, members of UK civil society have taken issue with the political responses of the UK Government in the post-Snowden era. In the Institute for Public Policy Research’s Study *Democracy in Britain*, Lord Macdonald argues that revelations about the GCHQ’s Project Tempora

point, perhaps, to an excessive and therefore damaging devotion to secrecy that appears to trump the right, even of parliament, to have a basic say in our security arrangements. The apparent manner of its conception and the government’s response to its being revealed is each troubling for the light it casts on questions of oversight and democratic accountability.⁴⁵

For Lord Macdonald, one of the most troubling aspects of what the Snowden disclosures revealed was that the GCHQ developed these capabilities while Government arguments to enact them in legislation were being successfully defeated in Parliament. As he notes, “[w]e are witnessing the creation of a very broad surveillance scheme by the backdoor – as successive governments have failed to persuade parliament that such schemes are justified or desirable – and a simultaneous growth in capacity and ambition on the part of GCHQ in the complete absence of debate, still less legislation.”⁴⁶ Lord Macdonald refers to recent government attempts to suggest that Tempora is implicitly authorized by RIPA as “deeply unconvincing,” questioning how it was possible that, “[i]f Chris Huhne is to be believed, the cabinet

⁴⁴ Moore, *supra* note 34.

⁴⁵ Guy Lodge & Glenn Gottfried (eds.), *Democracy in Britain: Essays in Honour of James Cornford*, INST. FOR PUB. POL’Y RES. (LONDON: UNITED KINGDOM) 173 (2014).

⁴⁶ *Id.* at 174.

and national security council did know [about Tempora]. They were never told."⁴⁷

Similarly, the House of Commons Home Affairs Committee released a seething report pertaining to the current UK mechanisms for intelligence oversight,⁴⁸ in which it criticized members of the British civil service – particularly the National Security Adviser and the head of MI5 – for refusing to give evidence.⁴⁹ While the Committee did acknowledge that the Justice and Security Act⁵⁰ made some changes to the Intelligence and Security Committee, it still concluded that,

[w]e do not believe the current system of oversight is effective and we have concerns that the weak nature of that system has an impact upon the credibility of the agencies accountability, and to the credibility of Parliament itself. Whilst we recognize the importance of limiting the access to documents of a confidential nature . . . engagement with elected representatives is not, in itself, a danger to national security and to continue to insist so is hyperbole.⁵¹

It also levied several criticisms towards the Investigatory Powers Tribunal and RIPA,⁵² and called it “unacceptable” that there was so much confusion around the work of the Intelligence Services Commissioner.⁵³ In doing so, they made a number of recommendations that will be considered further in this paper’s subsequent (and concluding) section on recommendations for change.

⁴⁷ *Id.* at 175.

⁴⁸ HOUSE OF COMMONS HOME AFFAIRS COMMITTEE, COUNTER-TERRORISM: SEVENTEENTH REPORT OF SESSION 2013-14, 66 [hereinafter *Home Affairs Committee 17th Report*], available at <http://www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/231.pdf>.

⁴⁹ *Id.*

⁵⁰ Justice and Security Act 2013 c. 18, available at <http://www.legislation.gov.uk/ukpga/2013/18/contents/enacted>.

⁵¹ Home Affairs Committee 17th Report, *supra* note 48.

⁵² *Id.* at 63-4, 70-71.

⁵³ *Id.* at 66.

III. CANADA AND THE UNITED KINGDOM – THE IMPACT OF THE SNOWDEN DISCLOSURES ON TANGIBLE LEGISLATIVE OUTCOMES

Andrew Clement has argued that, “[h]ow Canada responds to the NSA-Snowden crisis will define its identity and shape its future for decades to come.”⁵⁴ Unfortunately, if the early returns are a sign of things to come, Canada is not on its way to responding to the Snowden disclosures in any kind of comprehensive or definitive manner. Granted, in the first section of this paper, several attempts were made by members of Canadian civil society to point to a glaring lack of parliamentary oversight of intelligence activities. As noted in *A Crisis of Accountability*, a joint publication published in association with the University of Amsterdam’s Institute for Information Law and the Vrije Universiteit of Brussels, “[w]hile the net result has led to a greater understanding of CSEC’s activities and objectives, there has been minimal concrete movement towards reform aside from some early judicial proceedings.”⁵⁵ It is still unknown at this point whether either of the aforementioned constitutional challenges launched by the British Columbia Civil Liberties Association or the Canadian Civil Liberties Association will lead to fruitful reform. Despite a very active civil society, responses from the current Conservative government have been sparse.

Hopes for future tangible legislative outcomes are further called into question by the past track record of successive Canadian governments. For over a decade now, various iterations of Bill C-81 (which would enact a National Security Committee of Parliamentarians to provide *some* form of parliamentary scrutiny of intelligence activities) have died in successive Canadian parliaments, despite cross-party support in 2005 at the time of the bill’s inception. At that time, political instability associated with successive minority governments (and the corresponding dissolution of Parliament) could easily be assigned blame for the demise of Bill C-81. However, as Roy Notes, “[i]f partisan collaboration is rare and tenuous during minority regimes, it is quickly

⁵⁴ Clement, *supra* note 27.

⁵⁵ Davies, *supra* note 5, at 22.

forgotten once majority status is returned since the victors see little compelling reasoning in sharing unfettered power with its now-defeated opponents.”⁵⁶ The aforementioned current iterations of the bills (Bills S-220 and C-551) have been moving through Parliament at a snail’s pace, *despite* the impetus placed on them by the Snowden revelations. Even before the Snowden revelations, two separate judicial inquiries by Justices Iacobucci and O’Connor (both of which attracted significant public attention) called attention to an alarming lack of parliamentary oversight of intelligence activities in Canada. To date, the recommendations of these inquiries have still not been taken up by the Canadian government, despite the fact that the Standing Committee on Public Safety and National Security has reiterated their importance. While Canadians often enjoy debating the potential shortcomings of the US Congressional model, “other likeminded democracies have or are also forging more robust oversight and review mechanisms that are likely to prove increasingly consequential in balancing competing interests of security, secrecy and privacy in an environment of digital connectedness and information abundance.”⁵⁷ Canada can ill-afford to stay stagnant in a world that continues to evolve and produce new digital realities. Nor can it afford to hope that its civil society or its courts will spur the Canadian government to action.

To contrast, the issue in the UK is certainly not a lack of parliamentary oversight mechanisms of intelligence activities, but rather the appropriate means through which existing legislation and mechanisms should be refined. For the most part, the UK Government has responded with silence and secrecy, even going so far as to attack *The Guardian* and force them to destroy material that would be damaging to the GCHQ. It has been noted that, “Deputy Prime Minister Nick Clegg has ordered an ‘Obama-style’ review of intelligence agencies, to be led by the Royal United Services Institute, but the report will not even be released until after the May 2015 elections.”⁵⁸ As a result of this government response, Brown and Korff have argued that, “[i]t seems judicial intervention will be required to bring the UK’s legal framework back into

⁵⁶ Roy, *supra* note 19 at 8.

⁵⁷ *Id.* at 22.

⁵⁸ Davies, *supra* note 5, 70.

compliance with the Human Rights Convention.”⁵⁹ As noted above by Setty, even successful litigation may not bring about effective change because of the UK’s complex arrangements under RIPA, the European Convention for Human Rights and the Human Rights Act. As a result, “[w]ithout a Snowden-like disclosure to enable such review, or a strong commitment by the United Kingdom to abide by the human rights standards articulated at the European level, parliamentary oversight would be the key mechanism to protect against overreaching by the British intelligence community.”⁶⁰

If parliamentary oversight is to be the key mechanism to protect against future overreaching of the British intelligence community, then the recommendations put forward by UK civil society members, in particular Lord Macdonald and the House of Commons Home Affairs Committee, need to be taken seriously. While some may argue that the 2013 Justice and Security Act attempted to do just that,⁶¹ others are more skeptical. As Lord Macdonald notes,

[t]he Justice and Security Act passed last year handed marginally more power to the ISC, but did little to correct executive control over it. For example, each committee member is now appointed by parliament but must first be nominated for membership by the prime minister. The ISC now has the power to call for evidence or information from ministers and agencies; however, the means and manner in which information can be provided to the ISC must be outlined through a memorandum of understanding with the prime minister. In the

⁵⁹ Brown & Korff, *supra* note 37 at 6.

⁶⁰ Setty, *supra* note 39 at 28.

⁶¹ Home Affairs Committee 17th Report, *supra* note 48 at 62. “A number of witnesses to this inquiry took the opportunity to highlight the improvements to the Intelligence and Security Committee which were contained within the Justice and Security Act 2013. There were suggestions that the committee ought not to be judged on its previous failures but rather time ought to be given to see how it worked under the new regime.” *Id.*

light of the Snowden revelations, it seems that reforms in the J&S Act did not go far enough. Moreover, we also need to consider the extent to which RIPA can be said to remain an adequate mechanism for regulating surveillance activities.⁶²

Even if one accepts the argument that the Justice and Security Act was an attempt to respond to deficiencies in the oversight of intelligence activities, this paper has noted the concerns of several academics and civil society actors pertaining to various other pieces of legislation and mechanisms, including RIPA and the Investigatory Powers Tribunal, that have not been consequentially amended by that Act. These still require further attention on the part of the UK Government before any true tangible legislative outcome can be assessed to the Snowden disclosures.

IV. CONCLUSION – RECOMMENDATIONS FOR FUTURE CHANGE

Despite the apparent conclusion that neither the Canadian nor the UK government has responded to the Edward Snowden disclosures with tangible, consequential legislative changes, it cannot be said that these disclosures have had no impact. The revelations provided for by the Snowden documents have fundamentally changed public perceptions in both countries about how intelligence activities are carried out and have sparked civil society commentary amongst academics, judges, legal practitioners, interest groups and the media pertaining to how oversight of intelligence communities should be improved in the future. The immense energy and analysis that has gone into these various commentaries should not be lost. As Wesley Wark argues,

[w]hatever badge we stick to Mr. Snowden (and his media collaborators) may in itself not matter very much, and certainly will be dwarfed by the issue that he has called our

⁶² Lodge & Gottfried, *supra* note 45 at 176.

attention to. That issue is the practice, and future, of global electronic surveillance by state intelligence agencies. The ultimate verdict(s) regarding Edward Snowden the man will pale in significance alongside the verdict(s) on global surveillance.⁶³

With that in mind, this paper will now conclude by reiterating some of the most important changes that urgently need to be considered by both Canada and the UK going forward into a post-Snowden future.

For Canada, the most urgently needed change required is clear: the work of Bill C-81 needs to be fast-tracked through its current iterations, either Bill S-220 or C-551, so that the country may finally have some form of parliamentary review and oversight of intelligence activities. The Canadian government should not need to be implored to do this through damaging revelations of sensitive material, which will undoubtedly continue in the future (as noted at the outset of this paper, a new *Intercept* story pertaining to CSEC's spying was released only recently). Various successive Canadian governments have for too long ignored a glaring deficiency in Canada's overall national security apparatus. Two separate judicial inquiries have been commissioned (at no small expense to the Canadian taxpayer) and both have recommended the immediate need for additional review mechanisms. These recommendations have been further bolstered by the Standing Committee on Public Safety and National Security, and have been demanded by various civil society actors noted in this paper. The Canadian government is poised to introduce a whole new set of anti-terrorism laws that it has been working on since last year's attack on Parliament Hill.⁶⁴ There is growing concern that this new package of laws will actually increase powers of various

⁶³ Loch K. Johnson et. al, *An INS Special Forum: Implications of the Snowden Leaks*, INTELLIGENCE AND NATIONAL SECURITY, Vol. 29, 793-810, 810 (2014).

⁶⁴ Jim Bronskill, *Five Things to Know About Canada's New Anti-terrorism Measures*, CTV NEWS, Jan. 30, 2015, <http://www.ctvnews.ca/canada/five-things-to-know-about-canada-s-new-anti-terrorism-measures-1.2213071>.

intelligence and police agencies.⁶⁵ These concerns are further exacerbated by the fact that Canada has no genuine accountability mechanisms for the oversight of these agencies, or for its national security apparatus as a whole. It is simply irresponsible for the Canadian government to go forward with new counter-terrorism legislation without addressing this glaring gap in its current national security framework.

In contrast to Canada, the United Kingdom is significantly ahead in regards to existing infrastructure for parliamentary oversight and accountability of intelligence activities. That being said, there are a number of targeted recommendations for change that could significantly improve these oversight mechanisms, were they to be acted upon by the UK government. In particular, Lord Macdonald suggests six additional reforms: 1) The ISC should become a full joint parliamentary select committee; 2) it should be appointed by and responsible to both Houses of Parliament; 3) it should have stronger powers to obtain evidence. These should include the power to obtain information, by summons, from outside parties, lay experts, ministers and civil servants, as well as from security chiefs; 4) it should have an independent secretariat and independent legal advice, and it should have access to all information. Select committee procedures already allow the exclusion of material whose publication might be harmful and the disclosure of such material is a serious criminal offence; 5) it's chair should be a member of the opposition and should not be someone who has previously held responsibility for any of the security agencies; 6) Finally, we need to increase the level of institutional expertise to ensure that human rights are put at the heart of policy and strategies in this area, at a level that is more than rhetorical. We need to consider how such a committee could develop a wider role in educating parliament as a whole and, consequently, the public.⁶⁶

Similarly, the House of Commons Home Affairs Committee makes a number of recommendations that echo those of Lord Macdonald. They also believed that there were

⁶⁵ Andrea Janus, *Spy Service to Get Stronger Under Federal Bill*, CTV NEWS, Jan. 30, 2015, <http://www.ctvnews.ca/canada/spy-service-to-get-stronger-under-federal-bill-1.2213119>.

⁶⁶ Lodge & Gottfried, *supra* note 45 at 178-179.

several ways in which the ISC could be strengthened: 1) election of the membership of the Committee by the House of Commons; 2) the Chair of the Committee being a member of the Opposition and not a former Minister with responsibility for any of the agencies; 3) ensuring that the Committee has access to relevant expertise (for instance in terms of the technological aspect of the work carried out by the security and intelligence agencies); 4) allowing other Parliamentary Committees to scrutinize the work of the security and intelligence agencies.⁶⁷ The Committee also recommended that the Investigatory Powers Tribunal be legislatively compelled to produce an annual report on their work, containing at the very least the number of cases it has received and the outcome of cases determined in that year.⁶⁸ Finally, in regards to RIPA, the Committee argued that,

[g]iven the criticism which the Regulation of the Investigatory Powers Act is subject to, we believe that the legislation is in need of review. We recommend that a Joint Committee of both Houses of Parliament should be appointed in order to hold an inquiry with the ability to take evidence on the Act with a view to updating it. This inquiry would aim to bring the Regulation of Investigatory Powers Act up to date with modern technology, reduce the complexity (and associated difficulty in the use of) the legislation, strengthen the statistical and transparency requirements and improve the oversight functions as are set out in the current Act.⁶⁹

Although both Canada and the UK have very different starting points for how they should oversee their intelligence activities in the future, the motive behind both is the same. Civil society confidence in the ability of both governments to protect the privacy of their citizens reached an all-time low following the Snowden disclosures. As is noted by Bauman,

⁶⁷ Home Affairs Committee 17th Report, *supra* note 48 at 62.

⁶⁸ *Id.* at 63-64.

⁶⁹ *Id.* at 70-71.

[o]nly 5% of respondents in Canada trust government to guard their data, and this only rises to 7% in the United States. Whether in the United States, Canada, or the UK, it is clear from these results that a substantial proportion of the population are concerned about government surveillance and that there is a high degree of cynicism about what governments do with those data.⁷⁰

Members of civil society in both countries are doing what they can to compel their governments to act, but there is only so much they can do if their governments are unwilling. Both Canada and the UK need to start treating the Snowden disclosures as an opportunity to reassess how they collect intelligence, when they collect intelligence, who they share intelligence with and, perhaps most importantly, how they oversee the collection of that intelligence.

⁷⁰ Bauman, *supra* note 36 at 141.