# Terrorism, The Internet, and the Security/Privacy Conundrum

**John Adams** | February 2014

Strategic Studies Working Group Papers

CIC
Canadian International Council
Conseil International du Canada

CDFAI
Canadian Defence & Foreign Affairs Institute

## About The Author

John Adams is the former Chief of the Communications Security Establishment Canada and Associate Deputy Minister of National Defence. He was appointed in July 2005.

Adams graduated from RMC, earning a Bachelor of Engineering degree in Chemical Engineering in 1965. Adams is also a Rhodes Scholar after graduating, in 1967, with a Bachelor of Arts degree from Oxford University, in England, in 1967. He also graduated from the Army Staff College as well as the National Defence College. Adams joined the Canadian Forces in 1967 and served until 1993. He took on many roles, from command of 1 Combat Engineer Regiment in Chilliwack, British Columbia (CFB Chilliwack) to posts at National Defence Headquarters. He retired with the rank of Major-General.

After his retirement from the Canadian Forces, Adams was appointed Assistant Deputy Minister, Infrastructure and Environment, for National Defence. He left that post in 1998. From 2003 to June 2005, as Associate Deputy Minister and Commissioner of the Canadian Coast Guard, and from 1998 to 2003 as Assistant Deputy Minister, Marine Services and Commissioner, Canadian Coast Guard for Fisheries and Oceans Canada.



If you would like to download a copy of this report please visit **www.cdfai.org** or **www.opencanada.org**.

If you would like to be added to our mailing list or have questions about our publications please contact: contact@cdfai.org or info@opencanada.org.

ISSN 1925-4903

## Executive Summary

Terrorists make extensive use of the World Wide Web to train, to finance and to distribute information. The Internet is a facilitator 'par excellence'. Canadians and their government want a vigorous defence against any and all attempts by terrorists to threaten our way of life through the exploitation of the openness of the Internet and our enthusiastic embrace of all it has to offer. Accordingly, the Internet has become the theatre of operations in counterterrorism efforts.

To what extent should our nurturing of our capacity to confront the terrorist threat on the Internet be a concern for Canadians on the privacy front? How are our security and intelligence agencies governed? Are the accountability frameworks such that privacy will not be abused in the name of security? Are our laws and policies to ensure that metadata is afforded proper respect vis-a-vis the law despite it not being a private communication?

This paper examines Canada's cryptologic agency, the Communications Security Agency (CSEC), to address these questions/concerns. It concludes that CSEC seeks to ensure security and privacy in tandem, increasing the former while protecting the latter.

But this issue continues to be discussed. Why? This paper suggests that it has much to do with activities quite apart from CSEC. It points out that virtually all countries have sacrificed some privacy under other less weighty circumstances. As Bruce Schneier opines, "the Internet is a surveillance state. Whether we admit it to ourselves or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages it has access to. Facebook does the same; it even tracks non-Facebook users. Apple tracks us on our iPhones and iPads." Against that backdrop, suspicions regarding the CSEC have been heightened by the Snowden disclosures. Canadians want to be assured that their privacy is not being unduly sacrificed in the name of security.

The paper concludes with one option as to how it might be possible to convince Canadians that an appropriate balance of security and privacy exists.

## Sommaire

Les terroristes font grand usage de la Grande Toile (World Wide Web) pour entraîner, financer et distribuer de l'information. Internet est un facilitateur par excellence (en français dans le texte). Les Canadiens et leur gouvernement veulent une vigoureuse défense contre toutes les tentatives terroristes de menacer notre façon de vivre par l'exploitation de l'ouverture d'Internet et de notre adhésion enthousiaste à tout ce que celui-ci peut offrir. En conséquence, Internet est de venu le théâtre d'opération dans les efforts de contreterrorisme.

Dans quelle mesure la culture de notre capacité de confronter la menace terroriste sur Internet devrait-elle être une préoccupation pour les Canadiens quand il s'agit de préserver leur vie privée ? Comment nos agences de sécurité et de renseignements sont-elles gouvernées ? Les cadres de responsabilité sont-ils tels que la vie privée ne soit pas malmenée au nom de la sécurité ? Nos lois et politiques peuvent-elles nous assurer que les métadonnées soient traitées avec le respect qu'elles méritent devant la loi, même si ce ne sont pas des communications privées ?

La présente étude examine l'agence cryptologique du Canada, le Centre de la sécurité des télécommunications (CST), pour répondre à ces questions et à ces préoccupations. Elle conclut que le CST cherche à assurer la sécurité et la vie privée en tandem, en augmentant la première tout en protégeant la dernière.

Mais la discussion continue sur cette question. Pourquoi ? L'étude suggère que cela a beaucoup à voir avec des activités plutôt étrangères à la CST. Elle fait remarquer que virtuellement tous les pays ont sacrifié un peu de la vie privée sous d'autres circonstances moins lourdes. De l'avis de Bruce Schneier, « Internet est un état de surveillance. Que nous nous l'admettions ou non, nous sommes suivis à la trace tout le temps. Google nous suit, tant sur ses pages que sur d'autres pages auxquelles il a accès. Facebook fait de même ; il suit même des non usagers de Facebook. Apple nous suit sur nos iPhones et nos iPads. » Devant ce décor, les soupçons à l'endroit du CST ont été renforcés par les divulgations de Snowden. Les Canadiens veulent être assurés que leur vie privée n'est pas indûment sacrifiée au nom de la sécurité.

L'étude conclut avec une option selon laquelle il pourrait être possible de convaincre les Canadiens qu'il existe un équilibre approprié entre la sécurité et la vie privé.

In 2007, in the course of a discussion of the terrorist threat, I opined, "that the theatre of operations in the future will be the Internet and that we have to master it or we will pay the price."[1]

Even then terrorist organizations were making extensive use of the World Wide Web's (WWW) reach and anonymity to recruit, train, finance, share and distribute information. The WWW was a facilitator and enabler 'par excellence'.

As Gabriel Weinman and Daniel Benjamin argued in a 2004 article in The New York Times, "Islamist websites and chat rooms are filled with evaluations of current events, discussions of strategy and elaborations of jihadist ideology."[2]

This paper will review the terrorist threat today in the context of the importance of the WWW in understanding the jihadist movement's mindset and modus operandi.

Intelligence efforts to 'master' the Internet will be touched on, including the essentiality of that effort in combatting the threat. Metadata will be an example considered in the context of the security/privacy nexus.

Finally, the paper will conclude with some thoughts on the way ahead.

The current wave of terrorist activity that began in the late 1990s, Islamist extremism, is the security issue of our age. Its effects are felt around the world, spread by people who violently oppose any religion but Islam, not to mention democratic elections, equality for women, and many other features of the modern world. And Canada continues to be featured on al Qaeda's list of priority targets.

Similar to the United States, Canada has a large and growing Muslim population (currently comprising 3.2 percent of the total population) fueled primarily by immigration from a host of Muslim countries around the world.[3] I hasten to add, that the relative size of this valued diaspora is in no way cause for alarm; in Canada, the United States, the United Kingdom, and elsewhere, the concern is not the larger, peaceful community, but rather the very small groups of extremists scattered throughout the country. These extremist groups continue to present a serious national security threat as evidenced by the following sample of alleged offenses and thwarted plots:

- In the 2006 'Toronto 18' plot, 18 people considered to be loosely tied to al Qaeda were arrested for planning a series of coordinated attacks, such as detonating truck bombs, shooting in a crowded area, attacking prominent government buildings, and taking hostages.[4]
- In August 2010, three Ontario men—Hiva Mohammad Alizadeh, 30, Misbahuddin Ahmed, 26, and Khurram Syed Sher, 28—were arrested for terror-related activities as part of what became known as Project Samosa, and charged with making or possessing explosives and participating in the activities of a terrorist group, believed to have links with international terrorism.[5]
- In April 2013, Tunisian-born Chiheb Esseghaier, a Ph.D. student in Montreal, and Raed Jaser of Toronto, were arrested as part of an alleged al Qaeda in Iran plot to derail a New York to Toronto passenger train on the Canadian side of the border. A third man, Ahmed Abassi, was arrested in the US and faces terrorism charges there.[6]

1 Chris Thatcher, "Masters of a New Domain", March/April 2007, Vanguard Magazine, available at www.vanguardcanada.com.

2 Counter-terrorism: Canada's Counter-terrorism efforts: Assessment (Soufan Group), 25 July, 2013 available at http://soufangroup.com/tsg-intelbrief-assessing-canadas-counterterrorism-efforts.

3 'What the Terrorists Have in Mind: Bush is right that we need an 'offense.' But not this one," op-ed by Daniel Benjamin and Gabriel Weinmann, New York Times, 27 October 2004, p. A31. available at http://www.nytimes.com/2004/10/27/opinion/27benjamin.html?pagewanted=print&position=&_r=0.

4 Isabel Teotonio, "Alleged Toronto Terror Plot Detailed in Court", 31 Oct 2013, the star.com, available at http://www.thestar.com/news/gta/2008/03/26/alleged_toronto_terror_plot_detailed_in_court.html.

5 Andrew Seymour et al., "RCMP Say Project Samosa Suspects Were Preparing to Build IEDs, The Ottawa Citizen, available at http://www.ottawacitizen.com/news/RCMP+Project+Samossa+suspects+were+preparing+build+IEDs/3441574/story.html.

6 Greg Weston and The Canadian Press, 22 Apr 2013, CBC News, "Alleged al Qaeda Supported Plot Against Via Thwarted", available at http://www.cbc.ca/news/politics/alleged-al-qaeda-supported-plot-against-via-train-thwarted-1.1377031.

- On July 1, 2013, two Canadians, who were allegedly inspired by al Qaeda, were arrested in British Columbia for plotting to plant pressure-cooker bombs at British Columbia's provincial legislature headquarters on Canada Day.[7]

In addition to these domestic examples, Canadian security authorities are also concerned about terrorist attacks overseas that might target Canadian citizens and interests. Consulates, embassies, NGOs and private enterprises operating abroad are all potential targets.

As is true anywhere, it is difficult to accurately assess the ongoing threat of terrorism to Canadian interests. At the same time, and as the thwarted terrorist plots attest, that threat is both real and present and is believed to be largely al Qaeda inspired.

But how real and present? What is the threat of al Qaeda to Canada today? To answer these questions let us begin by answering the question, "What is al Qaeda?"

More than 10 years after the attacks of 9/11, there is no universally accepted definition of al Qaeda. However, it is generally accepted that the backbone of today's al Qaeda consists of its "general command" (sometimes referred to as AQ Core) in Afghanistan and Pakistan and its formal affiliates: al Qaeda in the Arabian Peninsula (AQAP), al Qaeda in Iraq (AQII), al Qaeda in the Islamic Maghreb (AQIM), al Shabaab in Somalia and finally, Jabhat al Nusra in Syria, which recently openly proclaimed its allegiance to Ayman al Zawahiri (bin Laden's successor). Collectively, al Qaeda's general command and the affiliates form an international terrorist network that is focused on both acquiring territory and executing terrorist attacks against the West. There are indicators within the public domain that al Qaeda's general command guides the overall strategy pursued by the affiliates and even sometimes gets involved in specific tactical matters. However, the affiliates likely enjoy a large degree of latitude in deciding how to run their day-to-day operations.[8]

Bruce Riedel opines that: "The coup in Egypt and the chaotic aftermath of the Arab awakening (Arab Spring) is only going to add more militants to this army of radicals. Failed revolutions and failing states are like incubators for the jihadists, a sort of Pandora's box of hostility and alienation."[9] The thinking is that the revolutionaries become frustrated with the failed attempt at democracy and faced with more of what had prompted the revolution in the first place, many of them turn to extremism as a last resort to rid themselves of dictatorship and the hardships that entails.

The news that al Qaeda leader Ayman al-Zawahiri and his man in Yemen, Nasr al Wuhayshi, were communicating and hatching plots to attack Western targets in the region should not have been surprising. Like any CEO of a multinational company, Zawahiri would be in regular communication, via the WWW, with al Qaeda's half dozen regional franchises—just as Osama bin Laden was before he was killed.

As Bruce Riedel has suggested, Egypt may well be the most critical piece.[10] Zawahiri seems to have calculated that the army coup in Egypt would radicalize millions of Muslim Brotherhood members, driving them into the embrace of al Qaeda. Al Qaeda has made unprecedented gains recently due to growing Sunni anger.

7 Alan woods and Wendy Gillis, "BC Terror Plot: Police Say Suspects Inspired by al Qaeda", 2 Jul 2013, thestar.com, available at http://www.thestar.com/news/canada/2013/07/02/bc_mounties_to_announce_terrorism_charges.html.

8 Thomas Joscelyn, July 18, 2013, Global al Qaeda: Affiliates, Objectives, and Future Challenges, available at http://www.longwarjournal.org/archives/2013/07/global_al_qaeda_affi.php.

9 Bruce Riedel, August 7, 2013, "The Coming of al Qaeda 3.0", Brookings Education, available at http://www.brookings.edu/research/opinions/2013/08/06-new-terror-generation-al-qaeda-version-3-riedel.

10 Ibid.

Today, the Al Qaeda Network is more geographically diverse than ever, [al Qaeda 3.0—if you like].[11] Its affiliates are fighting in more countries than at any other time before or after 9/11.[12]

For now at least, it is generally agreed that al Qaeda is focusing most of their efforts on the enemy close to home, "over there," rather than the faraway enemy in North America and Europe, "over here". But history would tell us that gains made "over there" could easily lead to a threat against westerners "over here". Examples include:

- In December 2009, AQAP placed a suicide bomber on board a Detroit bound plane. To that point many experts assumed that AQAP was only interested in attacking targets inside Yemen.[13]
- In May 2010, the Pakistani Taliban (TTP) dispatched a terrorist to Times Square. The TTP generally operate exclusively inside Pakistan and Afghanistan. And yet the group almost detonated a truck bomb in the heart of New York.[14]
- Then, as previously highlighted, in April of this year, there was the al Qaeda in Iran inspired plot to derail the New York-Toronto passenger train.[15]

These attempts demonstrate that while the al Qaeda Network is fighting for territory "over there", it remains a threat to North Americans "over here".

Furthermore, al Qaeda has been emboldened by events in the Middle East, particularly in Syria and Egypt. This renewed confidence was no doubt behind Al-Qaeda chief Ayman al-Zawahiri when, in a speech marking the 12th anniversary of 9/11 this year, he called for attacks on the United States and a boycott of the world's largest economy.[16] Success 'over there' breeds the confidence and the wherewithal to bring the fight 'over here'. It is estimated that 1000s of jihadists from all over the world, including dozens from North America, have made their way to Syria in support of the anti-Assad forces.[17] What better training ground for these 'foreign fighters', who will one day may make their way back home to become 'home grown terrorists' under the direction of al Qaeda's central command.

Like any other multinational organization, al Qaeda takes advantage of the WWW to spread its message for purposes of recruiting, training, financing, and sharing and distributing information (including on operational matters).

Canadians and their Government want a vigorous defence against any and all attempts by terrorists to threaten our way of life through the exploitation of the openness of the Internet and our enthusiastic embrace of all it has to offer. This is best delivered by an equally vigorous and multifaceted intelligence effort in support of counterterrorism.

So we must acknowledge the need for such intelligence apparatus, but to what extent should nurturing such capacity be a concern for Canadians on the privacy front? How are security and intelligence agencies governed? Let's examine Canada's cryptologic agency, the Communications Security Establishment Canada (CSEC) as an example.

11 Ibid.
12 Thomas Joscelyn, Op. cit.
13 Daily Mail Reporter, 28 Sep 2012, "Revealed: How Christmas Day Bomber's Exploding Underwear Failed to Detonate... Because He Had Worn Them for Three Weeks", available at http://www.dailymail.co.uk/news/article-2210190/Underwear-bombers-explosives-failed-detonate-worn-weeks.html.
14 Amir Shah et al, 11 Oct 2013, Washington Times, "Senior Taliban Commander Tied to Failed NYC Times Square Bomb Plot Captured", available at http://www.washingtontimes.com/news/2013/oct/11/senior-taliban-commander-tied-failed-nyc-times-squ/?page=all.
15 Greg Weston and The Canadian Press, Op. cit.
16 Ayman al-Zawahari, Speech marking the 12th anniversary of 9/11 this year, September 13, 2013, available at http://tribune.com.pk/story/603778/ayman-al-zawahiri-calls-for-us-attacks-economic-boycott.
17 Kristina Wong, Foreign Jihadists Surpass Afgan-Soviet War, Storm Syria in Record Numbers, 20 Oct 2013, The Washington Times, available at http://www.washingtontimes.com/news/2013/oct/20/foreign-jihadists-surpass-afghan-soviet-war-storm-/?page=all.

It must be said at the outset, that what CSEC can and cannot do is carefully detailed and circumscribed by law, Ministerial Directives, Ministerial Authorizations and policies. I quote from the applicable legislation:

> 273.64 (1) the mandate of the Communications Security Establishment is:
>
> (a) To acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
>
> (b) To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and
>
> (c) To provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.[18]

It is noteworthy that the legislation imposes the following limitations upon CSEC activities in any of their programs to deliver on this mandate:

> 273.64 (2) Activities carried out under paragraph (1)(a)
>
> (a) Shall not be directed at Canadians (anyplace in the world) or any person in Canada; and
>
> (b) Shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.
>
> (c) Activities carried out under paragraph (1)(c) are subject to any limitations imposed by law on federal law enforcement and security agencies in the performance of their duties.[19]

That is to say, CSEC cannot be used to circumvent any law applicable to the federal law enforcement or security agencies that the Establishment may be called upon to support.

Working in the global information infrastructure (GII) and targeting only non-Canadians, outside of Canada, CSEC acquires signals intelligence in support of counterterrorism. This information enables CSEC to anticipate and understand the capabilities of foreign terrorists and their intentions vis-à-vis Canada. Such information brings truth to the adage, 'forewarned is forearmed'. Legal and policy barriers arise when the foreign target contacts a Canadian. In this regard CSEC needs special provisions. These are provided for in the legislation:

> 273.65 (1) The Minister may, for the sole purpose of obtaining foreign intelligence, authorize the Communications Security Establishment in writing to intercept private communications in relation to an activity or class of activities specified in the authorization.
>
> Conditions for authorization,
>
> (2) The Minister may only issue an authorization if satisfied that:
>
> (a) The interception will be directed at foreign entities located outside Canada;
>
> (b) The information to be obtained could not reasonably be obtained by other means;
>
> (c) The expected foreign intelligence value of the information that would be derived from the interception justifies it; and
>
> (d) Satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.[20]

18 Canada's National Defence Act (NDA) Part V.1 273.64(1)(a), available at http://laws.justice.gc.ca/eng/acts/N-5/page-100.html#docCont.
19 Ibid. PartV.1 273.64(2).
20 Ibid. PartV.1 273.65(1).

All that to say, the Ministerial Authorization provides the legal authority if, in CSEC's gathering of foreign signals intelligence, they incidentally collect the communication of a Canadian or anyone in Canada, and at the same time it reinforces the need for robust policies and privacy protection measures to be in place.

The sanctity of Canadians' privacy is further ensured by a "culture of compliance" within CSEC. The then Commissioner of the Communications Security Establishment, Robert Décary, remarked in his 2012 Annual report, "I can say with confidence that … CSEC's Chiefs, during my time as Commissioner, have spared no effort to instill within CSEC a culture of respect for the law and for the privacy of Canadians."[21] Finally, regular reviews by the Commissioner are a confirmatory check on CSEC'S adherence to Canada's privacy laws, among others.

The Commissioner's mandate is included in the legislation:

> 273.63 (1) The Governor in Council may appoint a supernumerary judge or a retired judge of a superior court as Commissioner of the Communications Security Establishment to hold office, during good behaviour, for a term of not more than five years.
>
> (2) The duties of the Commissioner are:
>
> (a) To review the activities of the Establishment to ensure that they are in compliance with the law;
>
> (b) In response to a complaint, to undertake any investigation that the Commissioner considers necessary; and
>
> (c) To inform the Minister and the Attorney General of Canada of any activity of the Establishment that the Commissioner believes may not be in compliance with the law.[22]

The legislation goes on to say: "273.65 (8) The Commissioner of the Communications Security Establishment shall review activities carried out under an authorization to ensure that they are authorized and report annually to the Minister on the review."[23]

In summary, the legislation in combination with the review authority of the Commissioner of CSE sees to it that signals intelligence activities do not pose a threat to Canadians' privacy. I hasten to add, at this point, that one's international allies cannot be turned to for activities that cannot legally be done for oneself.

What about Canadian metadata; is it afforded proper respect despite not being a communication? Interest in this question has been heightened by some of the recent public disclosures by Edward Snowden.[24] The definitive answer to this question, in the case of CSEC activities, is an unequivocal yes.

Let us begin by explaining further just what metadata is. In this regard, Ann Cavoukian, Information and Privacy Commissioner, Ontario, Canada provides as good an explanation as I've found.

> Metadata is information generated by our communications devices (technical metadata) and our communications service providers, as we use technologies like landline telephones, mobile phones, desktop computers, laptops, tablets or other computing devices. It is essentially information about other information, in this case, relating to our communications.
>
> Metadata includes information that reveals the time and duration of a communication, the particular devices, addresses, or numbers contacted, which kinds of communications services we use, and at what geo-locations. All this metadata is collected and retained by communications service providers for varying periods of time, including by telecommunications companies and Internet Service Providers, for an array of business purposes.[25]

21 Robert Décary's 2013/14 Annual Report to Parliament, available at http://www.ocsec-bccst.gc.ca/ann-rpt/2012-2013/ann-rpt_e.pdf.
22 NDA, Op.cit., PartV.1 273.63(1).
23 Ibid. PartV.1 273.65(8).
24 The Guardian, "Edward Snowden", Oct 2013, guardian world news, Available at http://www.theguardian.com/world/edward-snowden.
25 Ann Cavoukian, July,2013, A Primer on Metadata, Ontario Government, available at http://www.ipc.on.ca/images/Resources/metadata.pdf.

You will note that there is no reference to the communication itself; that is, its content, in the definition of metadata. That is a key point to bear in mind when thinking about what level of privacy concern is appropriate in this case. It is noteworthy, however, that while it doesn't include private communications, metadata may well include personal information, which is not free from privacy considerations.

The fact remains, however, that CSEC's intelligence collection activities face outward, it is a foreign intelligence agency and is forbidden, by law, from targeting Canadians or anyone in Canada. Due to the nature of the WWW, incidental collection on a Canadian could occur, this is recognized and provided for through Ministerial Authorizations. This approach also ensures that the privacy of Canadians or anyone in Canada is protected. Furthermore the Commissioner of CSE conducts annual reviews on all authorizations to confirm this protection. Consequently, there is no security/privacy conundrum in CSEC activities. CSEC seeks to ensure security and privacy in tandem, increasing the former while protecting the latter.

But this issue continues to be discussed. Why? I suggest it has much to do with activities quite apart from CSEC. I think it safe to say that the train has already left the station with respect to all countries having sacrificed some privacy under other, less weighty circumstances. David Lyon highlights in his new book, *Liquid Surveillance* that; "social media sites depend for their existence on monitoring users and selling the data to others."[26]

He goes on to point out that, "we are in a new kind of social situation where visibility is taken for granted. Invisibility is no longer an option. There is always some eye watching us".[27] However, as Ian MacLeod points out, not all of these privacy compromises are bad: "Discerning our likes and dislikes can deliver convenience, comfort and efficiency, like the Amazon.com algorithm that informs buyers 'customers who bought this item also bought'".

The Ontario Lottery and Gaming Corporation has been praised by the Ontario Privacy Commissioner, Ann Cavoukian for its cautious and considered use of facial recognition technology to exclude self-identified problem gamblers from its casinos.

Google Flu Trends tracks the use of the search terms related to the flu, such as "flu remedy" or "influenza". The London Daily Telegraph newspaper reports the app can pinpoint outbreaks one to two weeks ahead of traditional flu watch surveillance. That can only be good.[28]

But some activities are an unwarranted threat to our privacy. As Bruce Schneier opines, "the Internet is a surveillance state. Whether we admit it to ourselves or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages it has access to. Facebook does the same; it even tracks non-Facebook users. Apple tracks us on our iPhones and iPads. One reporter used a tool called Collusion to track who was following him; 105 companies tracked his Internet use during one 36 hour period."[29] And on top of that, suspicions regarding the CSEC have been heightened by the Snowden disclosures. Canadians want to be assured that their privacy is not being unduly sacrificed in the name of security.

The lack of a forum to accommodate public discussion of this security/privacy conundrum has often been a criticism leveled at the intelligence community. Traditional open and transparent public debate of this and any other aspect of our security and intelligence operations has the very real downside of compromising the capabilities and trade craft of our agencies, which would enable the adversary to take steps to neutralize their effectiveness.

26 Zygmunt Bauman and David Lyon, "Liquid Surveillance: A Conversation, available at http://www.amazon.com/Liquid-Surveillance-Conversation-PCVS-Polity-Conversations/dp/0745662838/ref=pd_sxp_f_r.

27 Ibid.

28 Ian MacLeod, February 2, 2013, "Surveillance and Privacy", Ottawa Citizen,available at http://www.privacybydesign.ca/index.php/ispy.

29 Bruce Schneier, The Internet is a Surveillance State, 16 Mar 2013, available at http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance.

The need for operational secrecy certainly does not prevent security and intelligence agencies, like CSEC, from maintaining their obligations with a robust accountability framework, nor does it mean they operate irresponsibly. That said, it may be possible to bring assurances of that fact somewhat closer to the public domain. One approach could be to establish an all-party Parliamentary Intelligence/Security Review Committee. Its members, to include Members of Parliament and Senators, would be security cleared to ensure that they could be privy to all aspects of the intelligence and security operations thereby ensuring, on behalf of the House, the Senate and all Canadians that civil liberties are not being compromised in the name of security. This is an option that has been discussed for some time in Canada but never acted upon; perhaps the time to act is now.

## Strategic Studies Working Group

The Strategic Studies Working Group (SSWG)is a partnership between the Canadian International Council (CIC) and the Canadian Defence and Foreign Affairs Institute (CDFAI). The CIC absorbed the former Canadian Institute of Strategic Studies (CISS) upon the CIC's formation in 2008, and the CISS's original focus is now executed by the SSWG.