"ELECTRONIC COMMUNICATIONS INTERCEPTION AND PRIVACY:

CAN THE IMPERATIVES OF PRIVACY AND NATIONAL SECURITY BE RECONCILED?"

RESEARCH REPORT PREPARED FOR THE OFFICE OF THE PRIVACY COMMISISONER OF CANADA

BY:

PROFESSOR WESLEY WARK

VISITING RESEARCH PROFESSOR
GRADUATE SCHOOL OF PUBLIC AND INTERNATIONAL AFFAIRS
UNIVERSITY OF OTTAWA

March 2012

The author wishes to acknowledge the generous financial assistance provided under a Contributions Agreement by the Office of the Privacy Commissioner of Canada. Without this assistance the study could not have been undertaken or written. The views presented in this study are the author's alone and do not represent the official position of the Office of the Privacy Commissioner or of any government official or agency.

"ELECTRONIC COMMUNICATIONS INTERCEPTION AND PRIVACY: CAN THE IMPERATIVES OF PRIVACY AND NATIONAL SECURITY BE RECONCILED?" [1]

EXECUTIVE SUMMARY/ INTRODUCTION:

In a recent book that addresses the issues of privacy and national security, Daniel Solove makes two opening arguments. One is that "protecting privacy need not be fatal to security measures: it merely demands oversight and regulation." The second is that " we can't progress in the debate between privacy and security because the debate itself is flawed." [2] My study suggests that this first argument is too narrowly constructed. More than oversight and regulation is needed to protect privacy, though both are necessary ingredients. The debate between privacy and security is deeply flawed, to be sure, but the reasons for that situation are themselves complex and also embrace problems of secrecy, inadequate communication by government and lack of public knowledge.

My study is based on an examination of selected recent and contemporary developments in Canadian national security that have at their heart the practice of electronic communications interception and that hold serious implications for privacy protection. Electronic communications interception is a prominent tool of intelligence collection, one that has been profoundly affected by accelerating changes in the global and domestic security environment and by equally profound changes to technological capabilities. As the boundaries that traditionally separated domestic and international security threats have fallen away, with the advent of a globalized world, a globalised threat environment, and rising dangers posed by non-state actors such as terrorist groups, the demands on intelligence, and in particular on electronic communications interception with its free-ranging capacities, have grown commensurately. At the same time the on-going information revolution has opened up to surveillance a vast pool of data generated by private citizens. Demands for more and better intelligence to enhance security inevitably push intelligence systems into new streams of information; they also inevitably put new stresses and strains on both the idea and practice of privacy. [3]

The mission statement of one leading Canadian intelligence collector, the Communications Security Establishment [CSE] describes its mandate as including acquisition and use of information "from the global information infrastructure." [4] CSE has become a hybrid intelligence service, with a mission that includes foreign intelligence, cyber security, and the provision of technical expertise and assistance to domestic law enforcement and intelligence agencies. Its hybrid status is an adaptation to both the threat and communications environments that have emerged since the end of the Cold War. CSE has been subject to external review to monitor its compliance with the law and its adherence to privacy protections since 1996. Its status as a leading Canadian

intelligence agency is matched by the secrecy that surrounds its operations and by a high degree of public unawareness.

Part A of my study examines the public reporting by the Commissioner of the Communications Security Establishment, the one window that Canadians have into the activities of CSE. This reporting is surveyed over a twelve-year time frame, from the establishment of the CSE Commissioner's Office in 1996 down to the present. The CSE Commissioner stands as the principal watchdog guarding the privacy of Canadians in the context of the work of CSE. The Commissioner's Office, like CSE, has undergone considerable change, with a significant turning point marked by the 9/11 attacks and, in their aftermath, the passage of Canada's first Anti-Terrorism Act, which included a legal statute for CSE operations.

An examination of CSE operations and their impact on privacy, as seen through the eyes of the Commissioner's reporting, is followed here by a briefer study of the Canadian Cyber Security strategy, released in 2010 [**Part B**]. This strategy, among other things, shuffles the deck with regard to the government's organizational blueprint for tackling cyber threats. A new office was created within Public Safety, called the Canadian Cyber Incident Response Centre (CCIRC), whose mandate and capabilities are only generally defined and which will operate without any form of external review. The distinctiveness of the CCIRC from CSE, which also retains a cyber security function, is hard to discern and the impact of the operations of this new agency on privacy are open to question and deserve further scrutiny.

Links between the Cyber Security Strategy and the more recent announcement of a Canada-US "Perimeter Security" arrangement, are fashioned through the latter's emphasis on bilateral concerns about cyber security and arrangements for cross-border intelligence sharing. **Part C** of my study focuses attention on the deeply threaded insistence in the Perimeter Security Plan on the achievement of enhanced intelligence sharing across a wide range of issues. This insistence has a significant historical context, which is examined below; the historical context itself gives rise to concerns about how well past lessons have been learned as well as highlighting persistent sensitivity to the privacy impacts occasioned by cross-border intelligence flows.

The final component of my study, **Part D**, examines recently tabled and controversial draft legislation on "lawful access." Lawful access, too, has a history and carries with it past baggage about privacy protections threatened by measures that would allow private access by law enforcement and intelligence officials to Canadian communications without prior judicial authorization. While the debate over the latest version of lawful access legislation is only in its formative stages, my study seeks to shift the ground of this debate to consider the relative merits for both national security and privacy protection of regulated versus unregulated plans for intercept capacity on the part of private sector 'Telecom Service Providers' [TSPs] and government agents.

In the **Conclusion** to the study I try to highlight some areas of on-going concern and suggest ways to think about the essential ingredients for achieving national security goals

and privacy protection without threatening the core of either legitimate democratic aspiration. A tentative 'Yes' is provided to the question posed by the title of this study. The ramping up of electronic communications interception, a feature of the post 9/11 age of intelligence, can be accommodated alongside privacy protections with the right framework in place.

PART A.

The Communications Security Establishment, the CSE Commissioner, and the Protection of Privacy in a new Surveillance Age"

"I am fully persuaded that review agencies such as my own can make an important contribution to the on-going debate between the considerations of security and of privacy" CSE Commissioner Antonio Lamar, Annual Report, 2004-2005

In a new age of complex and variegated security threats and vastly expanded horizons for data collection, the Canadian Security Establishment (CSE) [5] stands out as a principal intelligence collector, as a government agency at the cutting edge of communications technology change, and as deeply secretive. In all those capacities it provides a useful, if uncommon, case study for exploring the central preoccupation of this study. CSE sits at the apex of concerns about electronic communications intercept and about privacy protections. Since the 9/11 attacks, CSE has seen its mandate transformed, while its still-young accountability regime struggles to keep pace. The one constant, amidst so much change, has been a professed adherence to the protection of Canadian privacy rights. [6]

The Communications Security Establishment, Canada's signals intelligence [SIGINT] agency, existed for a half-century in relatively untrammeled secrecy before it had to adapt to the existence of an external review body with a mandate to investigate and report on aspects of its operations. [7] This long history of secrecy presented challenges both for the CSE and for the review agency eventually established to monitor its compliance with the law. The review agency, the Office of the Commissioner of the CSE, was founded in 1996 and has its own, interesting pre-history. The CSE Commissioner found himself thrust, from the outset of his mandate, into a close inspection of the potential threats posed by Canadian SIGINT operations to provisions of the Privacy Act, prompted by the on-going electronic information revolution and the use of ever more sophisticated technological tools to allow CSE to chase its elusive communications targets. The CSE Commissioner's annual reports to Parliament provide one of the very few public windows available on CSE operations and their impact on the privacy of Canadians. The window is not of the 'picture' variety, and is attendant with problems of obscurity as the Commissioner's office struggles with secrecy and messaging considerations, and with review priorities, but it is all we have. It is also worth noting at the outset that the existence of an independent, judicial authority reporting in public on an annual basis on

Canadian SIGINT operations, with a special emphasis on privacy protections, makes Canada unique among our close SIGINT partners. [8] The source of this uniqueness is rooted in a combination of historical circumstances that were not replicated amongst our allies.

Genesis of the CSE Commissioner:

The genesis of an independent accountability mechanism for CSE can be found in four underlying factors, which operated cumulatively over a period of many years:

1. the repatriation of the Canadian constitution and the passage of the Charter of Rights and Freedoms in 1982;

2. the inspiration provided by the CSIS Act of 1984, with its dual accountability provisions for the Service;

3. the general climate ushered in by the end of the Cold War, which brought with it an increased demand for public knowledge of secretive security organisations and a greater governmental acceptance of the value of openness;

4. and, most unusually for Canadian SIGINT, which had enjoyed the deepest secrecy and public invisibility for most of its long life since 1946, sudden unfavourable and sensational publicity.

The McDonald Commission of Inquiry into the activities of the RCMP Security Service in the 1970s provided the first, detailed plan for review of the Canadian intelligence community. The McDonald Commission proposed two accountability measures that were meant to embrace not just the new civilian security service it envisaged [eventually to become CSIS], but the wider Canadian community. One accountability mechanism was to be provided by a small, independent investigatory body with its own expert staff, to be called the Advisory Council on Security and Intelligence. Its mandate was to cover all the security and intelligence agencies, including CSE. [9] The McDonald Commission also wanted to strengthen Parliament's [then non-existent] capacity to review aspects of the Canadian intelligence program and so proposed the creation of a Joint Parliamentary Committee on Security and Intelligence, similar to practice in Australia. [10] The Parliamentary committee remit would have covered CSE. In the event, neither of these recommendations was acted on by the government of the day. The idea of a Parliamentary committee was dropped altogether, following deliberations by a Senate committee chaired by Michael Pitfield. The notion of an independent body to review the security and intelligence committee was narrowed to become the Security and Intelligence Review Committee, whose writ would cover the Canadian Security Intelligence Service only. With both schemes in abeyance, further discussion of an external accountability mechanism for CSE was shelved for the remainder of the 1980s.

But the idea of an independent review of CSE didn't die completely and was raised again in the 1990 report issue by a special committee of the House of Commons that had been charged with conducting a review of the CSIS Act. In its report, entitled "In Flux but not in Crisis," the parliamentary committee cast its eye over the "wider dimensions" of the Canadian security and intelligence community and proposed a number of recommendations about accountability that reached beyond CSIS. It noted that CSE "clearly has the capacity to invade the privacy of Canadians in a variety of ways" and also recognized the secrecy dilemma regarding CSE operations. The Commons committee proposed two measures vis-à-vis CSE: that it be established by formal statute; and that the Security and Intelligence Review Committee's (SIRC's) mandate be broadened to include review of CSE's compliance with Canadian laws.[11]

These recommendations, as with many others proposed by the Commons committee, were not adopted by the government of the day. In its response, the government noted the array of internal accountability mechanisms that did exist with respect to CSE, beginning with Ministerial accountability to Parliament. It argued that a "broad accountability system for CSE is in place." But in a spirit of conciliation the government was willing to make at least a vague promise about the future: "Nevertheless such an accountability system can always be improved and the government has been considering providing the Minister of National Defence with some additional capacity for review of CSE." [12] What this additional capacity might be and when it might be forthcoming were left vague. A research paper produced for the Library of Parliament in 1993 noted that reforms to CSE accountability were still under consideration. [13]

A formal statute for CSE would, in the event, have to await the passage of the Anti-Terrorism Act in December 2001. Progress towards greater accountability for CSE was somewhat quicker—having been given a jolt by a series of unprecedented public revelations about CSE activities by former, disgruntled officials. In 1994 Mike Frost published SpyWorld: How CSE Spies on Canadian and the World, which contained dramatic and sometimes implausible accounts of CSE operations against a wide variety of targets, including Canadian citizens and politicians. In the fall-out from the Frost affair, Liberal M.P. Derek Lee introduced a private member's bill to make CSE accountable to Parliament. CSE chief, Stu Woolner, reflecting the shock and dismay within his agency occasioned by the Frost book, circulated a memo to his staff which stressed the law-abiding nature of CSE operations. [14] The Minister for National Defence, David Collenette, told Parliament that the government would not discuss intelligence matters but offered the reassurance that CSE did not target the communications of Canadians. [15]

One year later more unwonted tales from the CSE vaults made their way into the public domain. Former CSE analyst, Jane Shorten, in a series of televised interviews with CTV News, told Canadians that CSE has crossed the line into 'unacceptable' activities and was "going into the privacy of Canadians' communications." [16] Shorten seemed affronted by what she described as CSE activities in the economic intelligence field, including spying on allies, and by some of the collateral intelligence take this involved.

Not for the past twenty-five years had CSE had to endure any significant public exposure. The last significant spate of publicity had been occasioned by a CBC documentary, "The Fifth-Estate—the Espionage Establishment," which had aired on January 9, 1974. This public outing had led the government of the day to transfer, through an Order-in-Council, the then 'Communications Branch of the National Research Council' to the Department of National Defence and to re-name the organization the Communications Security Establishment. [17] The rationale was presumably to locate CSE in a more congruent Department where the security and anonymity of its operations could more easily be maintained.

This time around, the government moved to address heightened public attention and concern about CSE activities by announcing the establishment of an independent Commissioner, under the Inquiries Act, to review CSE's compliance with the law. So was born, in June 1996, the Office of the Communications Security Establishment Commissioner, initially for a three year period. [18] The Office of the CSE Commissioner was established through an Order-in-Council, perhaps with the intention of avoiding debate in Parliament on the precise nature of the Commissioner's functions.

Shortly after the creation of the CSE Commissioner's office, the Privacy Commissioner issued a classified report of a rare compliance audit into CSE functions. In referring to this audit in the OPC annual report, mention was made both of the complexity of the task and of the public allegations surrounding CSE activities. The Privacy Commissioner concluded, at the time, that CSE did operate in compliance with the Privacy Act, but urged enabling legislation for the agency that would describe its mandate, powers and operations. Succinctly put, the Privacy Commissioner thought enabling legislation and an accountability system would allow for "more light and less heat." [19] This general call was repeated by the Auditor General in a pioneering 1996 report on the Canadian Intelligence Community. [20]

The CSE Commissioner's Office would evolve over time under the guidance of successive Commissioners, each of whom put some individual stamp on the Office. Evolution would also be shaped by the Office's accumulated experience of CSE, and as longer-term planning for review took hold. Events, too, would shape the evolution of the Office; most notably, the terrorist attacks of 9/11. While somewhat artificial, the history of the Office of the CSE Commissioner, and of its reporting, can be broken down according to each individual Commissioner's tenure and approach to the task of divining risks posed by CSE operations to Canadians' fundamental privacy rights.

The Bisson Era (1996-1999): "All's Well"

In the first annual report issued by the new CSE Commissioner, The Honourable Claude Bisson noted that discussions on legislation for CSE were on-going and that he intended to study the matter further. He did say that he saw a "remarkable window" for a legislative statute for the agency. The 1996-97 annual report did affirm the Commissioner's opinion that CSE "has acted lawfully in the performance of its mandated

activities" for the period under review. Commissioner Bisson also found that CSE had not targeted "Canadian citizens or permanent residents." [21]

Commissioner Bisson repeated his finding on CSE lawfulness in his 1997-98 annual report, the first full report produced by his office. The Annual report was a strong endorsement of CSE policies (found to be "sound"), of CSE respect for the privacy of Canadians (a "cornerstone of CSE's SIGINT policies") and of CSE's focus on its foreign intelligence mandate. Commissioner Bisson not only pronounced himself satisfied that CSE did not target Canadian citizens or permanent residents, but went a little out of his way to refute specific allegations made by Mike Frost. These allegations included CSE's use of a link with the Norwegian SIGINT service to outsource the monitoring of communications between Quebec and France and the creation of a "French section" at CSE devoted to Quebec politics. [22] The CSE Commissioner stated flatly that "CSE does not target Quebec communications, or the Quebec sovereignty movement, and it does not have a 'French section.'" [23] This seemed to be an especially sensitive allegation for the former Quebec Court of Appeal judge.

Commissioner Bisson's mandate was renewed for a second, three year term by the Minister of National Defence in June 1999. The mandate remained essentially unchanged and the Office of the CSE Commissioner remained small, with a permanent staff of only two, augmented by contractors. Annual reports issued by the CSE Commissioner between 1998-99 and 2001-2001 continued to find that CSE acted lawfully and that it did not target the communications of Canadians. The 1998-99 annual report did comment on the efforts by the CSE Commissioner's Office to develop methods to test CSE databases and noted the problem of the "inadvertent" interception of Canadian communications since "absolute exclusion is technically impossible at this time." [24] The 1999-2000 annual report delved further into what was called the "ITS" (information technology security) role played by CSE. It noted, significantly, that CSE did not engage in tests of the defences of government information security systems, so-called "ethical hacking," as this "could reveal personal data with privacy implications." It also provided some insight into how CSE functioned within the "intelligence cycle" of government operations and of its partnership arrangements with allies. Again taking oblique aim at the claims in the Mike Frost book, Commissioner Bisson noted that Canada's SIGINT partners (the US, UK, Australia and New Zealand) had agreed not undertake collection on each other's behalf that would be illegal in the originator's country: "In other words, they do not do indirectly what they cannot do directly." [25]

The 2000-2001 Annual report was chiefly notable for its general recognition of the fast pace of change in information technology and the challenges this presented for CSE operations. Commissioner Bisson continued to promote the view that CSE "is well aware that it must continually upgrade its capabilities to screen out Canadian communications or risk acting unlawfully if it does not make every effort to do so." [26] The 2000-2001 Annual report also, for the first time, noted that CSE had begun to provide [unnamed] government clients with technical assistance. No mention was made of any privacy implications of such technical assistance.

So ended the run of the CSE Commissioner's annual reports in the years between the office's inception in 1996 and the 9/11 attacks. Commissioner Bisson provided brief and generalised accounts of CSE which uniformly affirmed its lawfulness and its attention to the need to protect the privacy of Canadian citizen and permanent residents. While the importance and complexity of CSE's task was recognized, no worrying flags were raised. The mid-1990s spate of revelations and charges relating to CSE, that had helped prompt the creation of the Commissioner's function, had died down and some of the charges made, in particular in the Mike Frost book, had been refuted by the CSE Commissioner. CSE had receded into the shadows. No new 'tell-all' accounts accounts emerged. Whatever anxiety existed in Canadian politics and society about CSE's intrusive powers had been damped down by the Commissioner's annual reports.

The 9/11 Effect

The Canadian government's response to the 9/11 attacks was to mark a watershed for CSE. CSE joined other elements of the Canadian security and intelligence community as resources and attention were massively shifted and intensely focused on the global terrorism threat. The passage of the 'omnibus' Anti-Terrorism Act (Bill C-36) in December 2001 provided CSE with the oft-called-for legislative statute, affirmed the role of the CSE Commissioner as a permanent watchdog over CSE's lawfulness, and explicitly re-shaped the CSE mandate to give it a significant counter-terrorism role. [27]

That CSE, for the first time in Canadian SIGINT history, was to have enabling legislation, as opposed to operating under provisions of a secret Order-in-Council, was in itself significant. That CSE would further tune its electronic ears to terrorist communications was inevitable. That its resources and budget would grow in the aftermath of 9/11 was necessary as it was Canada's premier foreign intelligence service in a security environment that would put an increasing premium on global information and on intelligence-sharing partnerships.

The Anti-Terrorism Act affirmed and codified what had become the tripartite mandate of CSE: to acquire foreign intelligence from the "global information infrastructure; " to help secure government communications infrastructure; and to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."

But at the heart of the amendments to the Criminal Code brought forth by the Anti-Terrorism Act was a new and unprecedented provision. This provision allowed CSE, under signed Ministerial authorization, to collect "private communications," defined in Canadian law as any communications that originate or terminate in Canada where such communications are attended with a reasonable expectation of privacy [Section 183 of the *Criminal Code*]. The Act laid out that such private communications could only be collected in fulfillment of either CSE's foreign intelligence or information security mandates and that the Minister would have to be satisfied regarding a set of listed conditions. These conditions were explicitly spelled out in the Anti-Terrorism Act. With

regard to foreign intelligence, the legislation specified that a Ministerial authorization to collect the private communications of Canadians could only be granted if four conditions were met:

a) the interception had to be directed [targeted] at foreign entities located outside Canada

b) the interception could not reasonably be obtained by other means

c) the interception was justified by its anticipated value

d) the privacy of Canadians would be protected and information retained or used only if it was essential to international affairs, defence or security

The criteria that had to be met to justify Ministerial authorizations in pursuit of CSE's ITS mandate were similar, although the value proposition was differently expressed. The criteria upheld the same conditions of prevention of harm to Canadian privacy, use or retention of private communications only when essential, and the absence of reasonable alternatives. The value proposition was not based on any balancing of means and end (anticipated value), but framed as a matter of "necessity" in order to "identify, isolate or prevent harm to Government of Canada computer systems or networks."

Given the arcana of signals intelligence, its relative unfamiliarity to Canadians, and the significant debates occasioned by other provisions of the Anti-Terrorism Act, especially relating to the framework definition of terrorism and some of the more extraordinary legal powers that could be invoked, such as preventative detention and investigatory hearings, it is hardly surprising that the section devoted to CSE got little attention and raised few concerns at the time. [28] Yet the government was certainly sensitive to the prospect that CSE's new operating statute would be misinterpreted or malignly misconstrued and went out of its way to explain the rationale for Ministerial intercept authorization while reassuring Canadians about the on-going strong protection of privacy. Allowing for the interception of Canadian communications without a warrant, no matter in what seemingly highly controlled and defined ways, required a careful explanation.

As Bill C-36 was being debated in Parliament, and in the country, CSE prepared an unclassified backgrounder on the proposed legislative changes. [29] This backgrounder surveyed the mandate of CSE, its history and its reporting structure. It noted the work of the Privacy Commissioner's 1996 audit and the on-going, affirmative reviews conducted by the CSE Commissioner since 1996. In a departure from past practice it gave out details of CSE's budget ($106 million in 2001/02) and workforce (c. 1000 staff). In highlighting the changes that the ATA would bring about for CSE it stressed two new elements:

1. that CSE would now have the legal authority to "collect the communications of a legitimate foreign intelligence target located abroad if those communications go into or out of Canada."

2. CSE's new legal powers would allow it to "monitor Canadian Government computer system and networks effectively in order to protect information and systems that are critical to Canada's well-being from mischief, unauthorised use or interference."

The first element retained its stress on CSE's foreign intelligence mission while expanding its capacity against foreign targets so as to not be shut out from their exploitation should communications lines reach into or travel from Canada. The second element was a little less clear, as the newness of CSE powers appeared to rest on an issue of "effectiveness," and a related potential need to pursue Canadian communications targets to achieve that end.

The Minister of National Defence, Art Eggleton, appeared before the House of Commons Standing Committee on Justice on October 23, 2001, to explain and defend CSE's proposed statue under the ATA. [30] He argued that the Ministerial authorization provision to allow CSE to collect Canadian communications in fulfillment of its foreign intelligence mandate was necessary to close a "serious gap" in Canadian intelligence capabilities. As an (hypothetical) illustration of this gap, Eggleton noted that under current laws "if a terrorist in Afghanistan is communicating with an individual at Pearson Airport, CSE is not allowed to acquire that communication." Eggleton also made a pitch for the new powers as improving Canada's status with its key intelligence allies: "I can tell you, these measures will be welcomed by these countries who will see them as evidence of our commitment to our close intelligence partnership."

On the need for Ministerial authorizations as an assist to CSE's information technology security mandate, The Minister was less explicit and offered no examples. He merely said that CSE was currently "restricted" in its ability to monitor the technical data on Government computer systems and networks that communicate with Canadians." The new law would authorize (in what ways was left unclear) "CSE to perform more effective monitoring of our computer systems and networks."

The Minister also took pains to explain how the new CSE powers would align with privacy protections, saying this was a matter of "paramount importance" to the Government. Eggleton argued that as Minister he would apply stringent tests before allowing interception, use and retention of Canadian communications for either foreign intelligence or ITS purposes. He also noted that the CSE Commissioner would review all Ministerial authorizations "to ensure that they are, in fact, authorized." What this might mean precisely and the degree to which it would involve the Commissioner interrogating Ministerial judgments and decisions would have to await interpretation by the CSE Commissioner. The review capacity was further complicated by the fact that the CSE Commissioner would report on such authorizations to the Minister who made them. [31]

The stage was being set for a subsequent period of mostly behind-the-scenes legal wrangling between CSE, the Department of Justice, and the Commissioner.

CSE's enabling legislation was duly passed as part of an amended Anti-Terrorism Act in December 2001. While changes were made to some core elements of the ATA, including the definition of terrorism, and a sunset clause attached to some of its more extraordinary provisions, the portions of the Bill that affected CSE were unaltered. CSE now had a new focus for its foreign intelligence collection efforts—the global terrorist threat—as well as enhanced powers to legally acquire information through Ministerial authorizations for the purposes of both foreign intelligence and protecting Government communications systems.

CSE's new, or vastly enhanced, focus on global terrorism was, for it, a voyage into the unknown. Identifying and acquiring terrorist communications would present a formidable challenge even in the context of cooperative work with SIGINT allies such as the US and UK with greater experience of the target. The challenge would be deepened as Canada's military commitment to Afghanistan was first established during 2001 and then hugely expanded after 2006 with our military deployment to Kandahar. The extent of foreign terrorist communications into and out of Canada was, probably, largely unmapped as of 2001 and the need to resort to Ministerial authorizations in future to pursue such networks unclear.

As for the strengthening of CSE's information technology security capabilities through Ministerial authorization powers, the only clue to the intent was provided by the comments in the CSE Commissioner's 1999-2000 annual report which noted that, at that time, CSE could not engage in so-called "ethical hacking" or test attacks on government communications system because it might open up private communications data protected under law. The implication of CSE's new legal mandate was that this prohibition might now be removed, at least in theory. Whether CSE was being unleashed not just to test government communications systems but to try to identify through proactive means the sources of illicit intrusion into government systems, whether based in Canada or abroad, or location unknown, remained unclear.

Despite the assurances provided by the Minister of National Defence, the privacy implications of CSE's new powers, even if largely overlooked in the debate over the ATA, were significant. The importance of the CSE Commissioner's review was increased commensurately even as the conditions of such review were, from the outset, problematic.

Post 9/11 review by the CSE Commissioner reflected a watershed in both the global and domestic security environment occasioned by the 9/11 attacks as well as the altered state of CSE's mandate and legal basis. On the occasion of the first post/911 review, the CSE Commissioner, still Claude Bisson, signaled the importance of the changes to the security environment and to CSE's legislative basis and took a deliberative approach by stating that: "it will take some time to fully assess the implications of the Anti-terrorism Act for my work." Commissioner Bisson noted "the responsibility of reviewing CSE activities

under Ministerial authorization is a significant one." [32] That the Commissioner was seized by the issue of the privacy implications of CSE's new mandate and powers was evident in his concluding comment that:

"Despite the enormity of events since my last report and the pressures now on Canada's security and intelligence community to provide information and produce results, to my mind the issue of privacy remains paramount." [33]

Commissioner Bisson's term concluded before he was able to fully report on the implications of Ministerial authorizations to collect Canadian communications. His last annual report was tabled in the House on June 13, 2003 (a year and a half after the passage of the Anti-Terrorism Act) and it could only be considered an interim reflection. [34] Commissioner Bisson, without noting the number of Ministerial authorizations granted or providing any details about them, did state that "information obtained from CSE indicates that the bulk of the communications intercepted under these authorizations are not in fact private communications (that is, they are not the communications of Canadians)." This was puzzling and left open the question of the need for Ministerial authorizations in these cases and the purport of Minister Eggleton's notion that the CSE Commissioner would be in a position to review whether Ministerial authorizations were, in fact, "authorized."

In other areas, Commissioner Bisson's final annual report commented on his examination of CSE operational support to CSIS, suggesting that such support would only be occasioned by CSIS's use of its Section 17 mandate to collect foreign intelligence in Canada, which would ultimately prove too narrow an interpretation of the technical assistance mandate. This issue would be taken up in subsequent reports by Judge Bisson's successors.

As in all of his previous reports, Commissioner Bisson ended his tenure by affirming that CSE had acted lawfully and had measures in place to protect the privacy of Canadians. There was a wistful note in conclusion that he was disappointed in never having been called as a witness before parliamentary committees to discuss his annual reports. But perhaps Parliament, like the public readers of his annual reports, found little to grapple with.

The Lamar Era (2003-2006): Getting to Grips with the new law and the new CSE

Commissioner Bisson's replacement was a retired Supreme Court Chief Justice, Antonio Lamar, whose greater legal experience and stature reflected both the new mandate accorded to CSE and the new review powers granted to the Commissioner in the Anti-Terrorism Act. Commissioner Lamar's first annual report (for 2003-2004), was tabled in Parliament in June 2004. Justice Lamar indicated he was seized by the significance of CSE's work, its challenges, and by its potential impact on Canadians. [35] He went some way beyond his predecessor in noting that actual number of Ministerial authorizations granted to CSE in the preceding year--there were 7 in total; five of which related to ITS.

This was the first snapshot provided to Canadians of the broad targeting of intercepts under Ministerial authorization and an indication that the bulk of these might well be directed at the communications security, as opposed to foreign intelligence, side of CSE's mandate. And for the first time, a problem was flagged. The CSE Commissioner noted what he called "certain weaknesses in policies and procedures related to these activities." Justice Lamar made clear that his intention was to be preventive, to identify risks and work with CSE to prevent them from turning into unlawful activities.

In commenting on Ministerial authorizations in his next annual report (for 2004-2005), tabled in Parliament in April 2005, Justice Lamar noted that his practice was to review Ministerial authorizations after they had expired, something that had not been clear in his first report. [36] The practice raised questions about the timeliness of reviews of MAs that might be renewed or 'rolled over,' and indeed about the general life span of Ministerial authorizations beyond their initial one year time line. What Justice Lamar did make clear was his priority in reviewing Ministerial authorizations, which was to be on CSE's foreign intelligence mandate as opposed to its ITS mandate. His rationale was two-fold: that the foreign intelligence directed activities had the greatest potential impact on the privacy of Canadians; and that Ministerial authorizations to collect Canadian communications under CSE's ITS mandate were prompted by requests from "client agencies whose systems and networks are being verified." Why this made such authorizations any less problematic, or the question of privacy protection any less significant, was left unclear. Commissioner Lamar reported on only three [expired] Ministerial authorizations, all of which pertained to CSE's foreign intelligence mandate. He did not reveal how many Ministerial authorizations had been granted in the previous year.

The vexed issue of just what the CSE Commissioner would review with regard to Ministerial authorizations came down to a question of whether he would focus on the "threshold conditions" for conducting such collection, as certified by the Minister, or instead on CSE's operational use of the authorization. Justice Lamar's explanation in the 2004-2005 annual report was somewhat opaque. He did indicate that he had provided the Minister with his interpretation of the MA provisions and had made "specific suggestions as to what could be done to remove ambiguities and to ensure common understanding of the operational application of these provisions." He also stated that he would determine "if CSE has met the conditions imposed in the MA." Both statements suggested the CSE Commissioner would restrict himself to reviewing CSE's deployment of Ministerial authorizations rather than the politically more sensitive terrain of their justification. Commissioner Lamar also indicated that his review of Ministerial Authorizations would be guided by "the intercepted private communications that CSE identifies to me as having been recognized and retained during the term of the authorization." While such a focus made sense given the restricted resources of the CSE Commissioner's office (which had now risen from a pre-911 level of two permanent staff to eight) and the need to zero in on areas of greatest potential harm to Canadian privacy, it also seemed to imply that the CSE Commissioner would pay less attention to CSE policies with regard to the treatment of Canadian communications inadvertently captured, or captured and not retained.

Commissioner Lamar ended his tenure with his Annual Report for 2005-2006. [37] During this period, CSE had come under renewed public attention as a spill-over from the controversy in the United States regarding media revelations about the development of a National Security Agency program to intercept US communications without a warrant. [38] These revelations prompted Justice Lamar to hold his own "extensive" inquiries about Canadian practices, including conversations with the chief of CSE, John Adams, who had taken over at CSE in July 2005 from his predecessor, Keith Coulter. Commissioner Lamar, without commenting directly on the NSA program, took the opportunity in his final annual report to implicitly highlight the differences between US and Canadian practice, including the fact that CSE's operations were established under legislation, that their lawfulness was reviewed annually, and that any interception of private Canadian communications required Ministerial authorization and was not left to the discretion of CSE itself.

While Justice Lamar indicated that his reviews of CSE activities conducted under Ministerial authorization reported no unlawful conduct he did note that important differences remained between his office and the Department of Justice over the "meaning of key provisions that influence the nature of the assurance that I can provide." The precise nature of this on-going dispute was not clarified. Commissioner Lamar urged the necessity of "seizing the next opportunity to make statutory amendments." It was something, he said, that had "bedeviled this office since December 2001."

That the secret dance between the CSE Commissioner and the Department of Justice might relate, at least in part, to the threshold conditions spelled out in the Anti-Terrorism Act for Ministerial authorization was, however, suggested by the Commissioner's concerns about the looseness of the connection between CSE applications to the Minister's office for authorizations and the foreign intelligence priorities established (on an annual basis) by the government. The closest that the CSE Commissioner came to surfacing the precise nature of his concerns came in the statement that "the lack of clarity in this regard has made it difficult for my staff to assess compliance with certain of the conditions that the legislation requires to be satisfied before a ministerial authorization is required." Too much reading between the lines is required here, but at the very least the legal impasse was worrying because it raised questions about whether CSE targeting might be too imprecise, might not sufficiently establish the absence of alternative recourse, or might not be able to identify the "essential" nature of the intercept operation—all threshold conditions spelled out in the CSE legislation. Above all, it left open the issue of whether CSE and/or the Minister were truly in a position to meet the requirement that "the expected foreign intelligence value of the information that would be derived from the interception justifies it." This was the ends-means balancing test that the legislation had provided for. If CSE intercept operations were only loosely tied to government foreign intelligence priorities, a shadow of doubt was cast.

In his final annual report, Commissioner Lamar also commented on his reviews of Ministerial authorizations for CSE ITS operations, a matter that in previous reports he had suggested was of secondary concern. In the 2005-2006 annual report, Commissioner

Lamar adopted a different approach, perhaps based on cumulative review experience. He stated "the authority to intrude on the privacy of Canadians in the course of protecting the government's computer systems and networks under ITS authorization is a sensitive matter." He urged CSE to improve its record keeping of such intrusions and indicated that he had asked his staff to monitor this issue closely in future reviews. [39]

The Gonthier Era (2006-2009): Unresolved Legacy Issues

Commissioner Lamar's successor was a brother judge retired from the Supreme Court, Charles Gonthier. Commissioner Gonthier inherited a well-established function and a staff experienced in dealing with the realities of the post 9/11 security environment, the ATA and an expanded CSE. He also inherited the legacy issue of concerns over the interpretation of Ministerial authorization powers. Like his predecessors he was faced with judgements about where the sensitivities lay with regard to privacy and lawfulness matters emanating from CSE's three core functions. Whereas earlier interpretations suggested that the overwhelming attention of the Commissioner's office should be placed on the foreign intelligence mandate, perhaps still reflecting the scandal driven revelations of the mid-1990s, greater experience and exposure gave rise to competing concerns about CSE's ITS and technical assistance mandates.

In the first year of Commissioner Gonthier's term, the House and Senate committees empowered with the mandatory review of the Anti-Terrorism Act were finally able to table their respective reports. Both reports picked up on concerns expressed in CSE Commissioner Annual reports about the lack of clarity surrounding the nature of Ministerial authorizations for CSE intercepts of Canadian communications. The House committee urged the government and CSE Commissioner to resolve the issue " as expeditiously as possible." [40] They also wanted some public explanation, if possible, of what the issue really concerned, something that neither the government nor the CSE Commissioner had been prepared to elucidate. Finally, in its brief section dealing with CSE, the House committee followed a recommendation made by the Privacy Commissioner that explicit reference be built into an amended CSE legal statute to require the agency's compliance with both the Canadian Charter of Rights and Freedoms and the Privacy Act.

The Senate special committee report on the Anti-Terrorism Act was only marginally more probing. [41] It picked up on a submission by former Commissioner Lamar that review of the nature of Ministerial authorizations would be assisted if a (legal) standard for CSE action was spelled out. The Senate committee argued that CSE interception of Canadian communications should be based on either a "reasonable grounds to believe…" or "reasonable grounds to suspect" standard. What the relevance of such a legal standard might be and exactly how it might be applied to the various threshold conditions stipulated in the Act for Ministerial authorizations with regard to foreign intelligence or communications security was not made clear. In particular, such a legal standard seemed to do little to clarify the balancing test of 'value versus risk' entailed in the foreign intelligence threshold condition; or the notion of 'necessity' laid down for ITS

authorizations. Where the Senate pressed ahead, beyond concerns expressed by previous CSE Commissioners, was in urging the government "in the interests of accountability and transparency," to have CSE report to Parliament on the number of Ministerial authorizations issued each year, and their general purpose (foreign intelligence or ITS). These figures were never explicit in CSE Commissioner annual reports, though CSE officials did advise the Senate committee that between December 2001 and April 2005 "no more than 20" ministerial authorizations had been issued and only 5 were still operational.

Neither the House nor Senate committee reports had anything to say about other aspects of CSE's new mandate. They offered no commentary on the challenges of CSE's counter-terrorism mission and said nothing about the third core function of the agency—providing technical assistance to other government departments. Neither report was prepared to take up the suggestion made by the Privacy Commissioner that intercept of Canadian communications should require prior judicial authorization. [42]

Commissioner Gonthier's first report was tabled in Parliament on June 12, 2007. [43] Not surprisingly, his first order of business was to reiterate his Office's long-standing concern with the lack of clarity in the legislation regarding Ministerial authorizations and the urgent need to make the required amendments to the Act. Perhaps rather optimistically, he suggested that the task should not be too onerous. He also spent time summarizing, in a neutral way, the findings of the Parliamentary reviews of the ATA, noted above.

Commissioner Gonthier then went on to discuss the findings of a legacy review (first established by Commissioner Lamar) of CSE provision of technical assistance to the RCMP. This third function of CSE had rarely been featured in previous annual reports and apparently had given rise to no concerns. Now, this more detailed study suggested that such operations might be problematic on two grounds, both potentially fundamental. The CSE Commissioner questioned whether CSE's foreign intelligence mandate actually authorized its support to the RCMP in connection with the Mounties' domestic criminal investigations. The annual report suggested that the Office would hold any judgment on lawfulness in abeyance until the matter was re-examined by CSE. The second problematic issue concerned CSE's authority to disclose personal information to requesting government agencies. This matter went to the heart of the CSE Commissioner's professed mandate to scrutinize the impact of CSE operations on the privacy of Canadians. But given the advisory function of the CSE Commissioner's Office and the non-adversarial approach established by Commissioner Gonthier's predecessors, all he could say on the issue was that he has recommended to CSE that it re-examine its lawful authority to "collect, use and disclose personal information to certain federal governments and agencies." [44] Commissioner Gonthier also recorded CSE's non-committal response, to the effect that further in-depth analysis by CSE and Department of Justice officials might be necessary. The issue was punted to the side-lines.

In his 2006-2007 annual report, Commissioner Gonthier also examined CSE's ITS mandate function and provided more detail on how the process of Ministerial authorizations for communications security probes worked. The CSE Commissioner

indicated that the process involved requests to CSE from concerned departments or agencies, after which CSE would seek a Ministerial authorization to allow them to "undertake a complete assessment of a department's computer systems or networks." Such authorizations were necessary because "personal information or private communications can be inadvertently intercepted with certain types of necessary testing." Here too, the CSE Commissioner found some problems, but they appeared to be matters of judgment about the retention of personal information, rather than more fundamental issues, as with technical assistance to the RCMP, that touched on legal authorities. [45] They appeared, in other words, fixable. This would be confirmed in the 2007-2008 annual report.

The pattern of rolling, ritual complaints about the ambiguity of the CSE legislation regarding Ministerial authorizations and the mystery surrounding how exactly the problem was defined by the CSE Commissioner's office persisted until the release of the annual report of 2007-2008. [46] The CSE Commissioner, perhaps prompted by sustained frustration and by the evident lack of progress on the part of the Government to address the issue, decided to seize the opening that had been provided by the Parliamentary review of the ATA. The House of Commons sub-committee that conducted the mandatory review of the ATA recommended that should the government fail to adequately address the dispute, the CSE Commissioner should make public his own assessment of the issue.

The CSE Commissioner did make clear his assessment, at least in part. Not surprisingly, it focused on the search for a more precise legal definition of terms in the Act, rather than the more politically sensitive terrain of the nature and upholding of the threshold conditions. But as we will see, greater legal precision also implicated, in the review process, the threshold conditions. Commissioner Gonthier indicated two of his principal recommendations. One called for more precision around the meaning of the term "activity or class of activities." This was in reference to section 273.65 (1) of the Act which stated:

"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." [*emphasis added*]

The CSE Commissioner believed that this definition must relate to the target of the CSE operation, not to the method of collection. [47] In other words, the CSE Commissioner believed that he had to be in a position to review the legitimacy of CSE operations on the basis of a clear identification of targets, which would inevitably lead to a consideration of whether the threshold conditions, including the value proposition, for granting of Ministerial authorizations had or had not been met.

Commissioner Gonthier also wanted to see a more precise, legal definition of the meaning of intercept and interception, either by reference to the existing Criminal Code definition or by introduction of a specified meaning in the ATA/National Defence Act.

Both principal recommendations, it should be noted, were also relevant to Ministerial authorizations to allow CSE to carry out its ITS mandate, although in a subsequent section of the 2007-2008 report, the Commissioner raised no concerns about Ministerial authorizations in his review of ITS activities. The suggestion here had to be that the ITS mandate was sufficiently focused on security assessments of specified departmental networks to remove concern about the precision of the legal language, especially in regard to targets and the nature of "intercept."

Without tighter definitions for the foreign intelligence mandate, Commissioner Gonthier argued, the CSE Commissioner had difficulty in adequately doing his job. The clear implication was that the review process and the assurances it offered to Parliament and Canadians about the protection of privacy rights was undermined.

The 207-2008 annual report offered greater clarity, and a renewed warning, but it left two mysteries. One was why the CSE Commissioner's Office had felt unable to spell out these differences previously; the other was why the government chose to stick obstinately to its interpretation. A gulf of some kind existed, but why it had to be shrouded in secrecy and why it existed at all, remained difficult to determine.

Commissioner Gonthier's final annual report was issued in June 2009, shortly before his death. [48] While much of Commissioner Gonthier's report concerned the legacy issue of ambiguity surrounding ministerial authorizations, and much of its was devoted to revisiting the methodology of his Office's work, some new notes were sounded. One important one concerned the sharing of intelligence gained through Ministerial authorizations with foreign allies. Although CSE had long been deeply embedded in an allied network of SIGINT agencies, the co-called "Five Eyes" partnership (Canada, the UK, the US, Australia and New Zealand) and foreign intelligence exchange was in many respects its life-blood, this was the first time in the history of the CSE Commissioner's office that the issue of sharing with foreign allies was publicly raised. The Commissioner reached no initial conclusions about this, beyond the recommendation that more information about such practices should be recorded and reported to the Minister. Commissioner Gonthier did note that "The sharing of information about Canadians is an area that my office will continue to examine." [49]

After Gonthier (2009-2011): 'On (Temporary) Auto-Pilot'

Commissioner Gonthier's initial three year term was extended by a subsequent year, but he died in July 2009. There followed a five month gap before a replacement was found. The new Commissioner, Peter deC. Cory, also a retired Supreme Court Justice, left the post after only a few months, to be replaced ultimately by a former Federal Court of Appeal judge, Robert Decary, in June 2010. Thus, in the short space of time between the summer of 2009 and the summer of 2010, three different CSE Commissioners occupied the post. The work of the Commissioner's Office continued, but leadership changes have

meant that no CSE Commissioner in the period following the death of Commissioner Gonthier was able to put any particular stamp on the Office's work.

The Annual Report of 2009-2010 was signed off on by Commissioner Cory just before he left the position at the end of March 2010. [50] He had been in place for less than four months. Inevitably the report was, in places, even more generic than usual. Much of the activity recorded was a carry over from previous work. The annual report did enunciate the Office's new approach to review of Ministerial authorizations under the foreign intelligence mandate. Because these authorizations continued, in the absence of any legislative amendment, to specify methods of collection rather than specific targets, the Office shifted to a more generic review—which they called "Horizontal review"--of practices common to CSE's conduct of foreign intelligence collection, including the selection of foreign entities, the sharing of reports with government clients and allies, and the retention/disposal of intercepted communications. The report also summarized the findings of an investigation launched by Commissioner Gonthier into CSE activities in the Afghanistan theatre from 2006 to 2008, which found little risk to private communications or information about Canadians but which extolled the overall value of CSE intelligence collection in this important war theatre for Canadian forces, diplomats and aid workers.

Arguably the most important study in the works for the CSE Commisisoner's Office, during this time of leadership churn, was that regarding foreign intelligence sharing with allies, first initiated during Commissioner Gonthier's tenure. The 2009-2010 annual report called this a "high-priority" review topic and gave numerous reasons why, including potential impacts on privacy and the nature of the controls placed on such sharing, which warranted examination. The study remained in the works as of 2010, and indeed was not completed in time for the 2010-2011 annual report.

The new Commissioner, Robert Decary, appointed in June 2010 for a three year term, was honest in expressing his lack of knowledge about CSE upon accepting office and indeed his skepticism about the degree of transparency and cooperation likely to be extended to his Office by CSE. In his first, and to date, only annual report, he noted that although he had experience on the bench of privacy and terrorism cases he "would never have imagined the extent of the activities of the Communications Security Establishment." He also confessed to have been quickly disabused about CSE recalcitrance, having been "impressed" and "surprised" by CSE and its Chief (then John Adams). [51]

Like Commissioners before him, Justice Decary used his annual report to reiterate the mandate of the Office of the CSE Commissioner and to touch on its methodologies and challenges. Commissioner Decary found himself particularly satisfied with "significant changes" that CSE had made in 2008-2009 to policies and procedures regarding its ITS function and noted that these addressed previous findings and recommendations made in a 2006 review.

Commissioner Decary also noted that following a temporary suspension of certain CSE operations in support of the RCMP and CSIS occasioned by a previous Commissioner's negative findings (reported in the 2007-2008 annual report), and an internal CSE review of policies and procedures, that CSE had instituted new approaches. CSE was now found to be in full compliance with the law and its use of its foreign intelligence mandate to support the RCMP and CSIS was deemed appropriate.

No details were provided as to the nature of the changes made regarding CSE's ITS or assistance policies and no explanation provided as to why the CSE Commissioner's Office found these changes so satisfactory.

The CSE Commissioner's Annual Report for 2010-2011 ended on a balanced note of combined "optimism and realism." That note faithfully reflected a 15 year period of review, in which Commissioners had consistently found a pattern of lawfulness and privacy protection on the part of CSE, while maintaining an expression of concern and vigilance about what the future might hold. A coda reiterated the on-going problem of delays with legislative amendments. Like his predecessors, Commissioner Decary hoped the government would act quickly—at the time of writing (March 2012) the hope remains forlorn. [52]

Part A Conclusions: The CSE Commissioner's Performance as a Privacy Watchdog?

The CSE Commissioner's function was established as a result of the cumulative impact of a number of factors, operating over a number of years, that prompted greater accountability for the Canadian SIGINT agency. One of these factors, and the one that may have provided the tipping point, was the sensational claims made by former CSE officers about CSE operations, including ones that touched on the privacy rights of Canadians. Since the Office's establishment in 1996, it has made itself the principal watchdog over the protection of Canadian privacy rights, as these might be impacted upon by one of Canada's lead agencies for electronic communications interception. The question that arises is whether the CSE Commissioner's Office has truly made the "important contribution to the on-going debate between the considerations of security and of privacy" suggested by the late Antonio Lamar.

The CSE Commissioner's Office has been, throughout its 12-year history, consistent in its broad approach to review of CSE. The approach has always focused on issues of propriety, rather than efficacy, reflecting the Office's mandate. Its powers are advisory only. The Office has stressed the need to build and maintain relations of trust between itself and CSE. It has taken what it calls a "proactive" approach to the risks involved in sensitive CSE intelligence operations, arguing that it can best fulfill its mandate by trying to identify problems and seek remedies through internal dialogue with CSE before they can become ingrained. The CSE Commissioner's Office has not positioned itself as an adversary to CSE and in Annual Reports has often gone out of its way to extol the cooperation of successive CSE Chiefs. It should be noted that Annual Reports from the

CSE Commissioner are uniform in finding that CSE has performed lawfully, even when such reports have marked some troubling issues.

The danger in such an approach, over time, is that the CSE Commissioner's Office can be viewed as co-opted and its assurances met with a degree of skepticism. The CSE Commissioner's reporting has also existed in an unfortunate vacuum when it comes to public policy debate in Canada. Its annual reports generate little media attention and are only rarely taken up by Parliament. The expert community that pays heed to these reports is tiny. The late CSE Commissioner Antonio Lamar implicitly recognized this problem when he attempted to create an outreach program for his office—by both involving the Office in public events and by encouraging outside experts to give presentations to his staff. That initial outreach effort was commendable but seems to have died on the vine in recent years, perhaps because of the unfortunate turn-over in CSE Commissioners.

An alternative to inevitable but probably unwarranted concerns about co-option, is to regard the CSE Commissioner's function as a glass half full. The CSE Commissioner's Office provides a public review capacity, however limited, and thereby lowers the secrecy walls. This in itself is a significant achievement. CSE Commissioner's annual reports provide an evidentiary source for those who are concerned about CSE operations and compliance with the law. The post 1996 review capacity is better than what preceded it (internal accountability only) by a far margin. The CSE Commissioner's function may well have had an impact on the culture of CSE itself—helping sow an appreciation of the need for lawfulness and respect for privacy on the part of CSE staff and leaders. There has also been an impact that spills over from the Commissioner's focus on propriety to matters of efficacy, in particular in regard to the Commissioner's calls for more efficient records keeping and database management, and refinement of CSE internal policies.

But what of the other half of the glass, the one not full? Bearing in mind that the CSE Commissioner's powers are advisory only, it nevertheless seems the case that the Commissioner's Office enjoys little clout in government. While there is evidence that it is listened to with respect by CSE, and a high percentage of its recommendations are adopted by CSE, it has been singularly unable to move the government to enact what it believes are necessary legislative amendments to the powers that govern CSE operations, above all regarding the sensitive issue of Ministerial authorizations.

As CSE Commissioners are wont to lament, their Annual Reports, even though tabled in Parliament as required, elicit little to no engagement by Parliamentarians or Parliamentary Committees. Some of the fault rests with Parliament, but some rests as well in the nature of the public reporting itself. As there are no security cleared Parliamentary committees, none of the classified reporting done by the CSE Commissioner is available to Parliamentarians.

The CSE Commission's annual reports suffer badly from opacity and from a tendency to provide only the most generic descriptions of CSE operations and the Office's response to them. That the CSE Commissioner's Office is simply a poor public communicator is

not a sufficient explanation. The charge that can be leveled here is that the CSE Commissioner's Office has been overly captured by official doctrines and cultures of secrecy, at the expense of its role as an information provider and source of Parliamentary and public reassurance. The most illuminating example of this is the failure of the CSE Commissioner's Office to provide any early explanation of the nature of its concerns about Ministerial authorizations. Even when it decided to be more open about this matter, in the 2007-2008 annual report, it did not provide a full explanation. It has, perhaps, valued its relationship with CSE and its reporting function to the Minster, more fully than it has valued its public obligation to provide a full accounting. The CSE Commissioner's Office is certainly constrained by national security confidentiality; but it has allowed itself to be overly constrained.

In developing its study of CSE over the years, the Commissioner's Office has also faced considerable challenges in penetrating the arcana of Canadian SIGINT, a highly technical, fast-evolving, sensitive and complex field of intelligence. Senior retired judges are not experts in this field and face steep learning curves matched against limited (generally three year) terms of office. The CSE Commissioner's staff may be expert [their qualifications are not made available in the public domain] but they are small. In the beginning, the Office's permanent staff was limited to 2; after 9/11 and the passage of the Anti-Terrorism Act it grew to 8. The question of where to focus the accountability effort was inevitably difficult. Understandably, given CSE's powerful self-image and perhaps some of the sensational accounts that surfaced in the mid 1990s, the tendency of the Commissioner's staff was to focus on CSE's foreign intelligence mandate as the area most likely to occasion risks to lawfulness and privacy rights. This focus left the other two parts of CSE's mandate-the ITS function and technical support to other government agencies—as secondary areas for coverage, sometimes attended by early assumptions that they involved lesser risks. Over time, the CSE Commissioner's Office was forced to broaden its accountability reviews and in the course of doing so discovered some problems with policies, practices and even legal mandates that pertained to these other core functions.

The one aspect of CSE operations that the Commissioner's Office awoke to in a very belated fashion concerned its intelligence sharing arrangements with foreign partners. CSE, from the outset of the Commissioner's function, was fully embedded in an alliance partnership, now known as the "Five Eyes," which could trace its historical roots back to the Second World War. Intelligence sharing with allied agencies was the life-blood of CSE operations and capabilities. Yet it was not until a decade had passed and the Arar Commission had reported that the Commissioner's Office began to take notice. In fact, the first mention of foreign intelligence sharing practices only surfaced in the 2008-2009 Annual Report and consisted of little more than a note about the need to monitor such activities in future. Yet the attendant privacy risks of CSE sharing details about Canadian individuals with foreign allies, according to unknown protocols, should have been self-evident from the outset and did not require the harsh lessons learned in a post 9/11 environment through the Arar and Iacobucci inquiries.

Finally, in surveying the CSE Commissioner's work over more than a decade of review there is one striking absence. No CSE Commissioner has ever singled out the practice of data mining for closer inspection in terms of its privacy impact, despite accumulated evidence in the public domain that data mining techniques are a prominent tool used by communications intercept agencies (as well, of course, as by private sector commercial operations). [53] The lone mention of data mining as a subject of interest appears in the Annual Report for 2006-2007, where Commissioner Gonthier noted that the Office was undertaking a review of CSE's "use of metadata," and that a report would be forthcoming in the next fiscal year. [54] No such report was apparently produced and no reference was made to it in the 2007-2008 annual report, or indeed subsequently. If such a study was prepared as a classified report for the Minister it is impossible to identify it as such in the listings provided by the CSE Commissioner's Office, and in any case the usual practice would be to refer to it in the annual report. Compounding concern over the missing 'metadata' report is an unusual undertaking to create a research institute housed within CSE to undertake "classified research in the areas of cryptology and knowledge discovery." The mission statement for the "Tutte Institute" describes its objective as to "support the Canadian Cryptologic Program and its international partners by providing leading-edge solutions to emerging complex problems." [55] The precise date of origin of the Tutte Institute is unknown, but its first director, Dr. High Williams, was appointed in February 2009. Research partnerships of the kind supported by the Tutte Institute can be vital to sustaining capabilities on the part of SIGINT and intelligence agencies, and have long been an established part of the activities of the U.S. intelligence community. That said, it is striking that the CSE Commissioner has paid no apparent attention to this development, at least in terms of providing reassurance that such a research institute is fully versed in CSE's privacy obligations and is capable of dealing with any risks to privacy attendant upon its work both in a domestic and international context.

The CSE Commissioner's Office has, over time, performed a valuable function in providing a degree of public reporting on CSE which otherwise would not exist and in helping inculcate respect for legal mandates and privacy risks within the CSE culture. The CSE Commissioner's Office has helped, in other words, keep CSE 'honest.' It has, on the other hand, failed to do as much as it could to keep the Canadian debate on security and privacy 'honest,' thanks to its cleaving too narrowly to an official culture of secrecy and by its inability to communicate its findings fully to Parliament and the public. The learning curve experienced by the CSE Commissioner's Office since 1996 perhaps had more bumps than it should, particularly owing to early assumptions about the over-riding importance of CSE's foreign intelligence mandate and by the obtuseness shown towards the risks attendant in CSE alliance relationships.

Justice Lamar's belief that the CSE Commissioner could make an "important contribution" to the debate over the needs of security and privacy was an honourable one; but the aspiration has yet to fully meet the reality. Privacy rights will always be under theoretical threat from powerful spy agencies, particularly in times of perceived crisis. There are four ways in which the theoretical threat can turn into a genuine one. The starkest way is if governments direct their spy agencies to perform unlawful and anti-democratic tasks. Fortunately, Canadian history has been largely free of such episodes.

Real threats to privacy rights can happen if the laws governing the operations of such a spy agency are insufficiently clear or inadequate to meet democratic requirements. It can also happen if the internal culture of a spy agency offers opportunities for unlawful activities at the margins. Finally, it can also happen, paradoxically, if under-informed or ill-informed publics begin to believe that a spy service threatens its rights, undermining that agency's legitimacy and threatening spill-over effects.

With regard to the current state of affairs, based solely on an examination of the CSE Commissioner's role and reporting as a privacy watchdog, three tentative conclusions are possible:

1. The legislation surrounding CSE, particularly with regard to Ministerial authorizations, is insufficiently robust and clear to protect Canadian privacy rights—and indeed insufficiently robust and clear to allow CSE to make its proper contribution to Canadian national security.

2. The lawfulness culture of CSE is sound

3. The Canadian public is under-informed (but not at the moment ill-informed) about CSE. CSE, one of Canada's most important spy agencies, possessing the capacity to have a significant impact on Canadian security and rights, continues, despite 12 years of public review, to operate in the shadows of the Canadian public consciousness.

To paraphrase a Privacy Commissioner of long ago, we are still seeking "more light" about CSE but maybe also need a little more "heat" to ensure that the government understands the importance of getting the legal standard for CSE operations, and for scrutiny of risks to privacy, right.

PART B:

The Canadian Cyber Security Strategy (2010) and its Implications for Privacy?

The debate over the threat posed by cyber aggression remains heated. While the security concerns prompted by cyber espionage and cyber crime seem well founded and empirically verified, those surrounding cyber war and cyber terrorism remain more speculative and disputed. [56] It was in this context of a rapidly evolving and unsettled threat environment that the Canadian government released its cyber security strategy on October 3, 2010, after a long gestation. [57] It followed the release of other national cyber security strategies by countries such as the UK, United States and Australia. The document is short on details and indeed short on any strategic outlook, noting the generic threat opposed by the different varieties of cyber aggression without indicating where priorities might lie. It purports to offer a blueprint for an integrated government

response, but surprisingly attempts to blend responsibilities for cyber protection ranged across a number of departments and agencies with a lead role ascribed to one Department, Public Safety, that 'owns' little of the response and protective capability itself.

The key protective element against the cyber threat that is housed within Public Safety is its "Canadian Cyber Incident Response Centre [CCIRC]." No details are provided in the document about the precise mandate, personnel strength, budget or capabilities of this unit. What the Cyber Strategy says is that the Cyber Incident Response Centre will "be the focal point for monitoring and providing advice on mitigating cyber threats and directing the national response to any cyber security incident." The conjunction is important here for this is actually two missions-a monitoring and advice mission and a national response mission. The monitoring and advice mission would seem, on the face of it, to usurp the role previously played for decades by the Communications Security Establishment (CSE) and provided for in its 2001 statutory mandate.

CSE gets only one mention in the Cyber Security Strategy, which does little to elucidate the potential overlap between its long-established ITS [Information Technology Security] function and that of the newly established Cyber Incident Response Centre. CSE is lauded in the document for its expertise, unique mandate and knowledge. The Cyber Strategy paper goes on to say that CSE will "enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems." What lay behind this marching order 'to enhance' remained unclear. No resource implications or outlays were explicitly provided by the Cyber Security strategy.

Governments are, of course, welcome to create over-lapping bureaucracies should they choose to do so. But the question in regard to cyber security of who is responsible for what does touch on important issues of national security capabilities, of accountability, and of respect for Canadian privacy rights. Without knowing the capabilities of the Cyber Incident Response Centre it is difficult to judge it in comparison to CSE. Yet it is hard to imagine that a new entity, short of engaging in serious manpower and resource robbing from CSE, could have an equivalent degree of cyber security capacity, or anything like it. What does distinguish the CCIRC from CSE, in a negative way, is the accountability regime. CCIRC will be accountable, in the usual Westminster way, to the Minister, and the Minister to Parliament, to the extent Parliament takes an interest. But unlike CSE, there is no established, external review body to monitor how it performs its mandate and the degree of lawfulness it shows, or how it acts to preserve privacy rights. We can expect no regular public reporting, or indeed any reporting, on the performance of the CCIRC.

Privacy rights themselves get only a passing mention in the Strategy, although arguably a major reason for wanting a cyber security capability would be to defend against intrusions on privacy. The Strategy simply mentions that it upholds "Canadian values such as the rule of law, accountability and privacy." Beyond the declaration, the details are missing.

Relevant to this study's concerns about the interception of electronic communications and the maintenance of privacy rights is the mystery of the apparent diminution of CSE's role from lead provider of ITS (or government cyber security) to a status of one partner among many. The many include, in addition to Public Safety and the Cyber Incident Response Centre, CSIS, the RCMP, Treasury Board, DFAIT, and the Department of National Defence. One telling indicator of the new, diffuse lines of operational authority is the idea that the RCMP (with new resources) would create its own "Cyber Crime Fusion Centre," which would respond "to requests from the Canadian Cyber Incident Response Centre regarding cyber attacks against Government or Canada's critical infrastructure." CSE was nowhere in the picture, even though they have the mandated authority to assist the RCMP in its criminal investigations.

It would be wrong to suggest, baldly, that this new blueprint for cyber security organization in the federal government was doing an end-run around external accountability. But that might well be the effect, even if unintended. Not only is the CCIRC without any external review agency, but many other components of the loose government network that is now meant to contribute to cyber security, also lack such bodies.

The decision to shift responsibility for aspects of cyber security to the CCIRC may also have reflected a desire to have a lead agency that could more easily work with non-governmental entities (such as private sector critical infrastructure) without having to deal with the "secrecy problem"--high levels of secrecy and security surrounding CSE operations. CSE was simply not a natural partner, whatever its level of expertise on cyber security issues, for other levels of government, the private sector and Canadian citizens. To the extent that the cyber security strategy puts considerable stock in cyber security "partnerships" between the federal government and other bodies, it needed a different lead agency. But the development of partnership arrangements between the government and the private sector carries its own risks when it comes to privacy protections. One example would be protection of private data in the course of what the strategy refers to as training and exercise programs partnered with the private sector. As the Cyber Strategy document has it, these partnership enterprises will be carried out without external accountability of the sort that would have been occasioned had CSE been left in a lead role.

Despite the Strategy's proclaimed intent to "create a culture of cyber safety whereby Canadians are aware of both the threats and the measures they can take to ensure the safe use of cyber space," no further public statements regarding implementation of the Cyber Security Strategy have been made since 2010. None, apparently, are planned. [58] The privacy implications of this new organisational arrangement prompted by the Cyber Strategy remain dangerously up in the air.

PART C

From "Smart Border" to "Perimeter Security": The Implications for Privacy of the Search for a Canada-US strategy for Border Security, 2001-2012

On February 4, 2011, the Canadian Prime Minister and US President issued a joint statement on a "shared vision" for perimeter security and economic competitiveness. [59] This vision statement would ultimately lead to the issuance of an "action plan" in December 2011. Neither document explicitly revisited the history of previous post 9/11 attempts to deal with the problems of border security and trade between Canada and the US, going back to the signing of the Smart Border Declaration in December 2001. All previous efforts at improving border security alongside border trade got merely a side-long glance, with references to "inertia and bureaucratic sclerosis" and the need to "up our game" to deal with common security threats.

Yet the history of a decade of effort deserves more than snide shots at government bureaucracies and a chummy sports metaphor. Past efforts contain lessons about where the hard challenges and dangers lie and remind us that we have been there before.

As I have written elsewhere, the 9/11 terrorist attacks created a profound security dilemma for Canada. [60] That dilemma was, in its most immediate form, a combination of fears about domestic security in Canada and concerns about how US reactions to an attack on their homeland would impact on Canada, the Canadian border and vital requirements for cross-border trade and travel. The comfortable myth of the 'longest undefended border' was transformed suddenly into a security nightmare. One of the top priorities for the Canadian government after 9/11 was to reach a renewed understanding with the United States about border security. The first fruit of that endeavour was the "Canada-US Smart Border Declaration," signed on December 12, 2001.

Reflecting the powerful security fears of the time, the Smart Border Declaration pictured Canada and the US working together to "develop a zone of confidence against terrorist activity." The underlying assumption was that no such zone existed, or if it had in the past, it had somehow been shattered. With confidence restored, the two countries could fashion (or re-fashion) a so-called "smart border..a border that securely facilitates the free flow of people and commerce; a border that reflects the largest trading relationship in the world." [61]

The Smart Border Declaration set out four "Pillars," which would guide work by both governments. These pillars involved: the secure flow of people; the secure flow of goods; secure infrastructure; and coordination and Information sharing. The basic tenets of the Smart Border Declaration were deep, mutual interests in security and trade, and efforts to achieve both by means of harmonization of policies and practices and close cooperation.

Following the declaration, an initial 30 point "Action Plan" was set out to describe various initiatives to be undertaken, structured according to the Four Pillars framework. Harmonized policies, cooperation against security threats, and intensified information sharing were involved in most of the 30 initiatives. Thus under the "Secure Flow of People" pillar, we find, for example, measures to share information on refugee and asylum claimants and on air travellers. Under the "Secure Flow of Goods" pillar we get proposals to explore joint border facilities, share customs data, and engage in joint analysis of container traffic. With regard to the "Secure Infrastructure" pillar, the action plan included joint work on key border points and trade corridors and binational threat assessments on trans-border infrastructure. Many of these initiatives posed at least potential threats to Canadian privacy rights. But it was the fourth "Pillar," on "Coordination and Information Sharing," and in particular action points 24 and 25, which called, respectively, for efforts to achieve "comprehensive and permanent coordination of law enforcement, anti-terrorism efforts and information sharing," and joint teams to "analyze and disseminate information and intelligence," that seemed to go to the heart of the new-model border as a 'zone of confidence against terrorism' and raised the most obvious potential for intrusions into Canadian privacy rights, in part owing to loss of sovereign informational control. [62]

Successive Privacy Commissioners paid close attention Canada's border security strategy and the general turn in Canadian security policy. George Radwanski sounded an initial tocsin of alarm in his annual report as federal Privacy Commissioner for 2001-2002. He worried out loud about the coming of "Big Brother," about the erosion of Canadian privacy rights through pressures for increased information sharing, and encouraged Canadians not to fall prey to American-style thinking about a "War on Terror." Radwanski's successor, Jennifer Stoddart, took a more nuanced position on the question of Canadian security policy, arguing that improved security could be achieved without destroying the fundamental values of Canadian society. Ms. Stoddart was concerned in particular about ramped up intelligence sharing and about the onward march of data mining in both the private and public sectors, but believed that the threats these developments posed could be corralled by establishing rules for the protection of personal information and with regard to its retention and sharing for national security purposes. The Privacy Commissioner voiced particular concerns about the Smart Border Declaration's emphasis on increasing intelligence sharing between Canada and the U.S., on the grounds that privacy protection systems in the two countries varied greatly and that Canada would lose control over information and its dissemination once it crossed the border. [63]

The Liberal government of the day remained unfazed by these criticisms. The National Security Policy paper, released in April 2004, contained as one of its three strategic objectives the prevention of any attacks launched from Canadian soil against an ally. The ally went unnamed but the reference was clearly to the United States. In a chapter of the Strategy devoted to Border security, the government extolled the Smart Border Declaration and Action Plan and urged that it be used as a model for other jurisdictions. [64]

A year after the release of the National Security Policy, the Smart Border model appeared to enjoy its first 'export' success, in the trilateral North American framework of the Security and Prosperity Partnership [SPP] announced at a leader's summit in Waco Texas. The SPP initiative also depended on working groups and action plans to implement detailed arrangements. But early skepticism about the true trilateral nature of the SPP and the generalized nature of proposals for common North American action on border security and trade were soon realized as the SPP found no traction except as a temporary annual leader's forum and ultimately withered away. [65]

The intelligence-sharing component of the Smart Border model took a hard and very public knock in the unfolding of the Maher Arar case, which realized some of the fears expressed by the Privacy Commissioner's Office about the dangers of unrestricted, cross-border information flows. Arar is a Canadian citizen of Syrian descent who was detained by the US authorities in transit in New York in 2002 and subsequently rendered to Syria, where he faced a year-long ordeal of harsh imprisonment and torture before being released by the Syrian authorities without charge and being returned to Canada. The Canadian government eventually and reluctantly bowed to public pressure in 2004 and called a judicial inquiry into the actions of Canadian officials in the Arar case. Justice Dennis O'Connor was appointed to lead the inquiry and to come up with recommendations for change. His report in 2006 called attention to the dangers of incompetent security investigations, undertaken principally by the RCMP, and to untrammeled intelligence sharing. He found that the mass sharing of unverified information on Arar with US authorities and the unmerited labeling of Arar and his wife as Al Qaeda members contributed significantly to his plight at the hands of US officials.

Justice O'Connor tried to spell out what he believed were the necessary principles that should underlay intelligence sharing. He was clear in his belief about two things: that intelligence sharing was vital to Canadian national security; and that intelligence sharing needed to be properly controlled. He believed the two principles were not at odds, but had to be kept in balance. He was not prepared to see the sacrificing of proper controls for the sake of greater information flows. Justice O'Connor stated:

"Information sharing is vital, but it must take place in a reliable and responsible fashion. The need for information sharing does not mean that information should be shared without controls…Nor does it mean exchanging information without regard to its relevance, reliability, or without regard to laws protecting personal information or human rights." [66]

At the same time, and perhaps responding to what he feared might be perceived as a recipe for unreasonable delay or for damage to the Canadian-US security relationship, Justice O'Connor believed that: "Controls [on information sharing] are meant to facilitate and promote the orderly flow of information, not to impede or stop it." [67]

Inevitably, it was left to Canadian security officials to translate these two principles into practice. At the RCMP this resulted in significant procedural and organizational changes to affect greater centralization of control over information sharing and to ensure that

official policies were understood and carried out. Whether changes at the RCMP, or elsewhere in the Canadian security and intelligence community resulted in slowdowns or friction with US counterparts over intelligence exchanges cannot be verified. Anecdotal evidence suggests that slowdowns did occur; while Canadian law enforcement and intelligence agencies continued to try to cope with relentless American pressure for high levels of information sharing.

In the meantime, the dynamic behind the original Smart Border Declaration and Action plan was losing steam for reasons that remain mysterious, but probably were not helped by the O'Connor Commission's damaging revelations about the Arar affair, by the overlaid distractions of the Security and Prosperity Partnership, by changes of government, and the advent of minority Parliaments. In the event, bureaucrats came to shoulder the blame for falling prey to inertia and "sclerosis." Not only did the leaders' statement of February 4, 2011, announcing a new "vision" of border security, place blame in this way, but it was happily seconded by two leading commentators on Canada-US relations . Tom d'Aquino, a former head of the Canadian Council of Chief Executives and Michael Hart, a University Professor and former senior trade negotiator, wrote in the Financial Post that three things had undermined progress with the original Smart Border plan: the failure to contemplate legislative changes; "bureaucratic inertia," which "wore out political commitment as the work plan became steadily captive to bureaucratic priorities and short-term political sensitivities;" and finally the absence of any animating "big idea." According to D'Aquino and Hart, both Prime Minister Harper and President Obama understood that the old effort was dead and that something had to be done. The commentators expected the two leaders to exercise a firmer whip hand over their respective bureaucracies and ministers this time around. [68] Roland Paris, in a parallel commentary, argued that bureaucratic obstacles arose in a climate of lessened urgency, as the shock effect of the 9/11 attacks slowly wore off and no second-wave strikes occurred. [69]

The ingredients that led, in 2011, to a renewed push to achieve security and trade flows at the Canada-US border involved new leadership commitments, the persistent concerns expressed by the business community about the economic impacts of a "sticky" border regime, and the ameliorative effects of the passage of time. Border policy could be made in a climate less touched by either urgency or its downside twin, loss of urgency. From the Canadian perspective, a new Border strategy could be made with a new political partner in the Obama administration, thus avoiding some of the domestic political pitfalls of deal-making with the Bush administration and also avoiding some of the ingrained mentality of senior Bush administration officials. The passage of time also allowed for some of the wounds occasioned by the Arar affair to heal or be forgotten. The passage of time even allowed for forgetfulness of another kind—that a Smart Border Agreement or Security and Partnership Agreement had ever been--thus allowing the Harper government to portray their Border initiative as something genuinely new.

What did not go away, in the intervening years between the first Smart Border Declaration and its 2011 cousin was the centrality of intelligence sharing to any

arrangement on Canada-US border/perimeter security, and with it concerns about impacts on privacy rights.

The "Perimeter Security and Economic Competitiveness" Action Plan, of December 2011, like its predecessor, The Smart Border plan, contained four "areas of cooperation" (the Smart Border action plan had called them "pillars"); like its predecessor it was also replete with detailed proposals for mutual initiatives, numbering 33 in total. [70] The specific "areas of cooperation," this time around, were identified as:

- Addressing threats early
- Trade facilitation, economic growth and jobs
- Cross-border law enforcement
- Critical infrastructure and cyber security

Initiatives under these areas of cooperation represented updates to earlier preoccupations that date back to the Smart Border Declaration and Action Plan. The one truly new feature was the emphasis on cyber security.

Proposals for enhanced intelligence sharing between Canada and the United States feature throughout the Action Plan, and in particular in the initiatives listed under "Addressing Threats Early." 'Upping our game' on intelligence sharing focuses on both people (potential agents of threat and cross-border travellers) and cargo; the privacy implications naturally being most prominent with regard to people. No baseline is indicated for the current status quo on intelligence sharing and no evidence is provided as to why this might be deemed unsatisfactory. The language of the document is all about improving intelligence sharing.

Several aspects of the planning for improved intelligence sharing are worthy of note. One is that the necessary context for securing value from increased intelligence sharing is identified as the achievement of a "shared understanding of the threat environment." [71] But the steps suggested to achieve this, in the incremental way of the Action Plan, will not take either partner very close to a genuine, mutual strategic threat assessment. The Action Plan talks instead about producing a "joint inventory" of existing intelligence work and a "gap analysis." Without a serious commitment to creating mutual understanding about the nature of the threat environment, intelligence sharing lacks a common framework and lacks an objective, and becomes a matter of information flows meant to serve distinctly defined national security concerns, while the continental partners might remain at odds about the broader meaning of the shared intelligence. The absence of an agreed, mutual assessment of the threat environment means that the loss of control of how intelligence is utilized once exchanged deepens concerns about its misuse and misinterpretation by partners on both sides of the border.

A second noteworthy feature of planning for increased intelligence flows involves "informal" sharing of law enforcement intelligence. [72] While the Action Plan notes that such "informal" exchanges must be consistent with the respective domestic laws of Canada and the United States, the concept of informal sharing is not defined and leaves a worrying impression of amnesia regarding the problems that emerged with similar examples of "informal" sharing in the Arar case. This worrying impression is deepened by a reading of a subsequent passage of the Action Plan, which encourages an examination of "impediments" to cooperation, including applicable laws, in a spirit of allowing for the "widest measure of cooperation possible."

A third feature of the Action Plan that depends on intelligence sharing is the proposal to create "integrated teams" for intelligence and law enforcement purposes, drawing on the "Shiprider" model. [73] Shiprider is a program that allows for the joint manning of Coast Guard vessels in shared Canada-US waterways such as the Great Lakes and the St. Lawrence Seaway. These joint manned vessels share marine enforcement duties and, of course, information flows. While pilot projects only are planned, it must be noted that such operations bring intelligence sharing very close to its application in law enforcement—they are, in effect, a form of integrated, intelligence-led policing.

In the new emphasis in the Action Plan on protecting shared Cyber infrastructure, improved intelligence sharing again comes to the fore. In particular, the Plan calls for the "enhancement of real-time information sharing between operation centres" and for joint briefings with the private sector. [74] As noted in the discussion on Canada's Cyber Security Strategy, the Canadian Cyber Incident Response Centre, the applicable Canadian node for real-time information sharing on cyber threats and attacks, is a new organisation stood up within Public Safety Canada and, unlike the Communications Security Establishment, operates without any form of external review.

One question that arises in regard to all the initiatives planned under the Perimeter Security agreement concerns accountability. The Action Plan promises a joint, pubic annual report on implementation progress, with the first report scheduled for release by the end of 2012. It will remain to be seen how detailed these annual reports might be, but it is unlikely, on the basis of past experience with the Smart Border Declaration and the Security and Prosperity Partnership, that they will be very revealing. The opportunity for Parliament or the public to understand and challenge some of the initiatives, especially with regards to the implementation of new measures for intelligence sharing may well be limited, which will put on onus on existing review agencies, including the Security Intelligence Review Committee, the RCMP Public Complaints Commission, the Commissioner for the Communications Security Establishment and the Privacy Commissioner to attempt to scrutinise border security developments as closely as possible. [75]

The Privacy Commissioner's Office will have an unusual stake in scrutiny of the perimeter security strategy, owing to the pledge to create a joint statement of Canada-U.S. privacy principles. According to the document both countries are committed to

"protecting privacy in all the initiatives we are undertaking." The Action plan makes a pointed connection between strong privacy protections and intelligence sharing:

"Responsible sharing not only demonstrates respect for the rule of law but also facilitates and promotes the flow of accurate, relevant and necessary information to address threats to national security and conduct law enforcement while respecting citizens' civil liberties." [76]

This is very much in the spirit of the O'Connor Commission recommendations and holds out a hopeful sign that lessons have been learned from past mistakes that will be applied to the intended dynamic of increased intelligence sharing. The Privacy Commissioner's Office will have an important role to play in assessing the joint privacy principles agreed upon by Canada and the U.S. While the Office will not, it would appear, be an actor in shaping the agreement, the agreement itself, once codified, may provide a powerful tool for reviewing the compatibility of border security initiatives with privacy protections. The privacy statement is scheduled to be completed by May 30, 2012 and will, presumably, be made public, though that is not explicitly guaranteed in the document.

PART D.

Once More Into the Breach: 'Lawful Access' Version 2012

Bill C-30, formally entitled "The Investigating and Preventing Criminal Electronic Communications Act," was tabled in Parliament on February 14, 2012. [77] C-30 is the latest incarnation of attempted legislation, the history of which goes back over a decade, to update Canada's laws concerning aspects of the mandated interception of electronic communications. [78] The current bill has already run into political difficulties in the House of Commons and a firestorm of public criticism and, at the time of writing, has been sent to Committee for further study and possible amendments.

Given that the final shape or fate of the legislation cannot be known, the purpose of my study is to briefly examine the alleged security benefits that would accrue from the passage of such legislation, and the protections provided for privacy rights. It thus addresses the critical question how such legislation benefits security while protecting privacy, rather than competing approaches that talk of balancing security against privacy rights, or defining tradeoffs.

The security benefit of the legislation is set out broadly and initially at **3.0** and focuses on the "capability" of telecommunications service providers [TSPs] to "enable national security and law enforcement agencies to exercise their authority to intercept communications." In more detail C-30 provides a regulatory framework that compels large TSPs to install surveillance capacities on their systems (set out at **7.0** of the draft legislation), and that provides for government scrutiny of these TSP capabilities (sections

33 to **38**). The draft legislation also provides a regulatory framework for how designated police, and intelligence officers from CSIS, may access basic subscriber data and the nature of the data [so-called data points] they may request (sections **16-17** of the draft legislation).

The surveillance capabilities required of TSPs provide for both current and future operations designed to allow real-time monitoring, the isolation of specific communications, the identification of those communications, and capacity to allow for simultaneous interceptions by a number of different agencies [all at **7.0**].

Government scrutiny of TSP surveillance capabilities is to be accomplished by the use of government-designated "Inspectors" who would be officially certified and would have wide-ranging powers to engage with TSPs, including entering premises, examining documents and equipment, testing and examining systems and reproducing signals [principally at **33.0** to **34.0**]. TSPs are required to cooperate with government Inspectors and face monetary penalties should they fail to do so, or should they fail to meet the regulated standards [sections **39** to **63**].

Under the draft legislation, police officers designated by the Commissioner of the RCMP (or a senior officer), by the head of a provincial police force or by the Director of CSIS (or a senior official) may, armed with a written request in furtherance of their duties, require a TSP to provide six identifying data points regarding intercepted communications [section **16** of the Act]:

Name
Address
E-mail address
Telephone number
Internet protocol [IP] address
Local service provider identifier

These powers are extended in an emergency to "any" police officer [section **17**]. [79]

With regard to the system of regulation that the Act sets out, it is worthy of note that broad ranging powers and considerable latitude are reserved to the government through Orders-in-Council (which may be secret) to set out the details of the Act's implementation [section **64**]. While the intent of this section may be to allow for flexibility in the application of new powers and to keep up with future technological changes, it is nevertheless sweeping and may impose challenges for accountability and review.

The draft legislation does provide for the protection of privacy rights and for accountability of the use of new surveillance powers, which is the other side of the coin.

The first mention of the protection of privacy rights comes in watered-down form in the initial definition of the purpose of the Act, where it refers to the creation of TSP intercept

capabilities "without unreasonably impairing the privacy of individuals." [**3.0**] Nowhere in the draft legislation is a strong statement made about observance of the Privacy Act. The system of checks on the 'unreasonable impairment' of privacy consist of a number of measures including the creation and retention of records by police and intelligence officers who utilize the powers of the Act [section **18**], internal audits [section **20**] , and external audits conducted by the Privacy Commissioner in the case of the RCMP and the Security Intelligence Review Committee in the case of CSIS [Section **20.4** and **20.5**]. In addition, the draft legislation envisages a five year Parliamentary review of the Act [**67**].

Government agency records-creation and retention is an important feature of the draft legislation and vital to any effective and fair system of regulation. Less specific and satisfactory is the imprecise nature of the internal audit process—no specific time frames are set out and no locus or level of responsibility for these audits identified. External audits will clearly be assisted by the mandated reporting requirements, but the external audit process is fragmented across multiple review bodies.

In addressing the issue of the security benefits to be achieved through the draft legislation, two questions need to be asked. One is whether a regulated system is better for national security than an unregulated one? The other is whether the proposed regulated system is sufficient to the purpose.

There can be little doubt that intercept of electronic communications is and will continue to be a valuable law enforcement and intelligence tool for protecting national security. It also seems undoubted that the fast pace of technological change will continue, with attendant challenges for national security agencies. Greater competition in the marketplace for TSPs also creates a scenario of variegated intercept capabilities. Law enforcement and intelligence agencies require a predictable and, to the extent possible, stable system of intercept capabilities.

The current situation in Canada is that we have an unregulated system of TSP surveillance capabilities, alongside an unregulated system of government law enforcement and intelligence access to basic subscriber information from TSPs. As Michael Geist has identified, there is a very high level of compliance on the part of TSPs with government agency requests for subscriber information, but this compliance involves an informal system in which no detailed records are required to be kept by both government and private sector agencies and no checks are conducted. [80]

The question of relative security benefit thus becomes a question for the future about whether a regulated or unregulated system is most likely to deliver the required predictable and stable platform for interception.

An unregulated system may continue to function well, if informally, as at present. It may be more cost-effective, especially for the government; it may impose fewer impediments to free-market competition; and there may be benefits in the informal partnership between private and public sector in terms of keeping pace with technological change. Governments may not always be at the cutting edge of security practices when it comes

to cyber space and any regulated system that looks to government-imposed standards may be second-rate. Canadians seem culturally sensitive to "Big Brother" intrusions and their seeming avoidance may also have political benefits which could accrue to the security file in terms of sustaining public legitimacy on the part of law enforcement and intelligence services.

What an unregulated system cannot provide, in terms purely of security benefit, is a stable and predictable intercept capability on the part of TSPs. It might, but there is no guarantee and the possibility of significant gaps in capability, especially in the future, must be entertained. Against that possibility is the phenomenon of private sector self-interest in data mining. TSPs of all capacities will have, as part of their business model, an interest in being able to retain, use and manipulate basic subscriber data. An unregulated system is thus self-regulated to a considerable degree by the private sector. Ultimately, whether such self-regulation is satisfactory speaks to philosophies of government and politics.

Another way of measuring the relative security benefit of regulated versus unregulated systems is to consider the question of 'discipline.' In an unregulated system, the 'discipline' around intercept capabilities for both government and private sectors is provided by general lawfulness requirements, performance requirements and, for the private sector, by the demands of a competitive marketplace. In the sort of regulated system proposed by the draft legislation, the 'discipline' takes on some more distinctive and concrete forms. These include creation, retention and reporting requirements for government officials; the creation of a class of government "inspectors," and the demands of internal and external audits as a check on both efficacy and propriety. [81] This, it would seem to me, is a more serious form of 'discipline' and one more easy to make consistent and sustained over time. It has a spill-over security benefit in terms of increased professionalism, sustained law-abidance, and the building and maintenance of a lawful law enforcement and intelligence 'culture' based on acknowledged societal values. The discipline involved in the legislative regulation may come at a cost in terms of bureaucratic requirements and even careerism, but the cost would seem to be outweighed by the benefits. Parallel benefits accrue to the private sector TSPs.

In my view, a regulated system for TSP intercept capabilities and government access does not necessarily outperform, in terms of security benefits, an unregulated system. Where they differ is in terms of providing for a measured discipline in the conduct of intercept capabilities. A regulated system provides for a higher degree of discipline around conduct and thus offers more reassurance about security deliverables.

If the relative security benefit of a regulated system comes with the provision of discipline, the question then shifts to the protection of privacy rights. [82] An unregulated system is not an invitation to criminality. It is not immune to internal and external audits, and must meet all the requirements of the law and of the Privacy Act. But a higher level of risk to privacy protections exists in the unregulated system. What a regulated system allows for is greater scrutiny of intercept capabilities and government access, especially through mandated reporting and audit practices. With greater scrutiny comes the promise

of more lawfulness and more checks on the erosion of privacy rights in what will be an on-going struggle between the temptations of cyber space usage and traditional norms of privacy.

What this amounts to is the rather Orwellian proposition that a "Big Brother" regulated system for intercept capabilities and government 'lawful' access is potentially better for security and better for privacy. [83]

This does not mean that the current legislation offers the most palatable "Big Bother" measures, or the most effective in terms of security discipline and privacy protections. Bill C-30 is complex legislation, one reason why it will have a hard passage and why previous efforts have failed. [84] If the overall scheme of a regulated system is preferable to the current un-regulated practice, the details of the new scheme warrant close attention. [85]

In particular, the following general recommendations are advanced:

1. a stronger statement about, and rationale for, the preservation of privacy rights and the requirements of security needs to be included in the language of the Act.

2. more specificity needs to be provided about the chain of command for government records retention and reporting

3. a specified minimum time table for internal audits needs to be provided.

4. External audit agencies should be required to share their findings and, where appropriate, collaborate on investigations.

5. Management of the regulatory system through Orders in Council should be kept at a minimum and wherever possible should be opened to public scrutiny

6. The Minister of Public Safety should be required to table an annual report on the performance of the regulatory system including detailed statistics on access to basic subscriber information on the part of the RCMP and CSIS.

7. The Auditor General should pay close and on-going attention to the costs involved in implementation of the Act, particularly with regard to subventions paid to TSPs for required upgrades in intercept capabilities.

CONCLUSION:

The answer to the question posed in the sub-title of this study—"Can the Imperatives of Privacy and National Security be Reconciled"—is yes, in theory. To move from theory into the realm of practice requires several ingredients, as this study has demonstrated.

These ingredients include strong accountability mechanisms, of the kind that the Commissioner of the CSE is designed to provide. The CSE Commissioner has consistently made privacy protection a central element of the scrutiny of CSE's lawfulness. Yet the performance of the CSE Commissioner's function has been hamstrung by an inability to communicate to the Canadian public and by the long-drawn-out battle to bring sufficient agreed clarity to CSE's legal mandate with regard to the intercept of private communications under Ministerial authorization. The CSE Commissioner's office has also been late to investigate the key issue of CSE intelligence sharing with foreign partners, and seems to have left data mining off its research agenda altogether.

Strong accountability aids in the creation of a second important ingredient in finding paths to reconciliation between national security and privacy demands. Accountability helps foster and sustain appropriate normative cultures in law enforcement and intelligence agencies. These cultures, such as that which seems on display at CSE, are a product of education, training, leadership, professionalism and even careerism. They are not fostered by external accountability mechanisms alone—but strong accountability is a factor and in its absence problems can arise. For that reason the lack of external accountability that surrounds the new office of the Canadian Cyber Response Incident Centre is regrettable.

The Canadian Cyber Security Strategy released in 2010 illustrates a third ingredient in binding national security and privacy protections together, namely the value of clear and coherent statements of national security objectives and of the delivery of national security goods. The Cyber Security Strategy was, to its credit, a first public step, but it was far being clear and coherent. The picture it drew of cyber threats was overly generalized and un-prioritized; and the proposed organizational structure to meet such threats was byzantine in nature. The Cyber Security strategy lacked, unfortunately, a strong statement about privacy protections and introduced a new agency that would operate both within government and in public-private partnerships, without external accountability.

The Perimeter Security Strategy, of even more recent vintage, offers a clearer statement of strategic objectives but unfolds such a large menu of intended actions that the overall strategic objectives of "Perimeter Security" are easily lost to sight. Happily, if inconsistently, the Perimeter Security action plan pays much more attention to privacy issues than does the Cyber Security Strategy and even promises a joint Canada-US declaration on privacy protections. The challenge posed by Perimeter Security lies in the necessity of preserving informational sovereignty while advancing other cooperative goals. The embrace of enhanced intelligence sharing as a cornerstone of Canada-US

border relations threatens privacy protection in the absence of a belief in informational sovereignty and in the absence of a sustained effort to arrive at a common strategic threat assessment.

The latest iteration of "lawful access" legislation to enable intercept capabilities on the part of private sector Telecom Service Providers and access to intercepts by law enforcement and intelligence personnel provides a strong, if unsurprising, reminder about the importance of good laws. In the case of Bill C-30, the legislation at issue is regulatory in nature and my study argues that both national security and privacy protections are better advanced by a system of regulation of intercept capabilities, rather than reliance on unregulated and more informal processes. That said, the current draft legislation, which may undergo substantial changes before enactment, or may die on the Parliamentary order papers yet again, is far from satisfactory in terms of clarity, precision, openings for accountability and strong statements about national security needs and privacy protections.

Strong accountability, normative cultures, clear strategic statements, ordered bureaucratic mandates, loyalty to a concept of informational sovereignty, and good laws are the key ingredients that can allow for the reconciliation of national security requirements and privacy protections.

Finally, linking all of these ingredients, is the need for public knowledge. It can be delivered through accountability mechanisms such as the CSE Commissioner, through strong strategic statements, and through good laws. One overarching weakness in the Canadian system is the poor delivery of public knowledge through all these media. Privacy is threatened in the absence of an appropriate level of knowledge about national security institutions and practices, in the absence of clear government statements and actions in its defence, and in fuzzy law-making.

[1] I wish to acknowledge the generous financial support of the Office of the Privacy Commissioner of Canada without which this study could not have been undertaken or completed. The arguments and analysis contained in this study are the author's alone and do not constitute an official view of the office of the Privacy Commissioner of Canada. I would like to thank, in particular, the Manager of the Contributions Program for the OPC, Francois Cadieux, for his assistance, understanding and patience.

[2] Daniel J. Solove, Nothing to Hide: The False Tradeoffs between Privacy and Security (New Haven: Yale University Press, 2011), p. 2

[3] One indication of this is provided in a speech by the then Deputy Director of National Intelligence in the U.S., Donald Kerr, who argued in 2007 that a new distinction needed to be drawn between privacy, which required protection, and 'anonymity,' which did not. See "Remarks and Q & A by the Principal Deputy Director of National Intelligence, Dr. Donald Kerr," 2007 GEOINT Symposium, San Antonio, Texas, October 23, 2007. *In the author's possession.*

[4] CSE's mandate is outlined on the service's website at www.cse-cst.gc.ca

[5] The Communications Security Establishment has, since 2007, been referred to officially as the Communications Security Establishment Canada (CSEC). For uniformity of reference and to avoid anachronisms, I will refer to it throughout this paper as the Communications Security Establishment (or CSE).

[6] For a brief survey of CSE's pre 9/11 history, see Martin Rudner, "Canada's Communications Security Establishment, from Cold War to Globalization," in Matthew M. Aid, and Cees Wiebes, eds., Secrets of Signals Intelligence during the Cold War and Beyond (London: Frank Cass, 2001), 97-128.

[7] Stuart Farson provides a detailed account of the use of secret Orders-in-Council to establish post-war Canadian SIGINT, and of the various efforts made over the years to establish greater accountability for the agency. See Stuart Farson, "So You Don't Like Our Cover Story—Well We Have Others: The Development of Canada's Signals Intelligence Capacity Through Administrative Sleight of Hand, 1941-2000" in Robert Mernzies et al, eds., (Ab)Using Power: The Canadian Experience (Halifax: Fernwood Press, 2001), 78-94; for a thorough study of the national security accountability system in Canada see Reg Whitaker and Stuart Farson, "Accountability in and for National Security," Institute for Research on Public Policy [IRPP], Choices, vol. 15, no. 9 (September 2009); available online at www.irpp.org. The study's general comments on the role of the CSE Commissioner appear at pp. 27-28

[8] The accountability mechanisms and review systems of Canada's close SIGINT allies vary considerably. In the United States, the operations of the National Security Agency are overseen by Congressional Committees and by an internal Inspector General. In the UK, the Government Communications Headquarters falls under the review mandate of the Security and Intelligence Committee of Parliamentarians, appointed by the Prime Minister and operating in the so-called "ring of secrecy." In Australia, the Defence Signals Directorate (or DSD) is reviewed by a joint committee of Parliament dedicated to the Australian Intelligence Community.

[9] Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police [McDonald Commission], Freedom and Security under the Law, Second Report, vol. 2 (Ottawa, August 1981), pp. 883-91; see also Stuart Farson, "In Crisis and in Flux?"

Politics, Parliament and Canada's Intelligence Policy," Journal of Conflict Studies, 16, no. 1 (1996)
[10] McDonald Commission, pp. 896-902
[11] Report of the House of Commons Special Committee on 'The Review of the Canadian Security Intelligence Service Act and the Security Offences Act,' Ottawa, September 1990, p. 153 and recommendation 87.
[12] Government of Canada, "On Course: National Security for the 1990s—the Government's Response to the House of Commons Special Committee on the Review of the Canadian Security Intelligence Service Act and the Security Offences Act," 25 February 1991, pp. 54-55.
[13] Philip Rosen, "The Communications Security Establishment: Canada's Most Secret Intelligence Agency," Parliamentary Research Branch, Library of Parliament, Background Paper BP-343E, September 1993, pp. 10-11
[14] The Woolner memo was quoted in the Ottawa Citizen by columnist Greg Weston on November 11, 1994. Reproduced in Frost, Spyworld, postscript, pp. 271-72.
[15] Frost, Spyworld, postscript, p. 271
[16] Quoted in Nomi Morris, "Canada's Spy Agency from the Inside," Maclean's, September 2, 1996, reproduced in The Canadian Encyclopedia online (www.thecanadianencyclopedia.com)
[17] Rosen, "The Communications Security Establishment," pp. 3-4; James Littleton, Target Nation: Canada and the Western Intelligence Network (Toronto: Lester and Orpen Denys, 1986), pp. 96-97
[18] Farson, "So You Don't Like Our Cover Story," credits Parliamentary pressure, "mainly from members of the Sub-Committee on National Security," for the government's decision to establish the Office of the CSE Commissioner.
[19] Privacy Commissioner of Canada, Annual Report to Parliament, 1995-96
[20] Auditor General of Canada, "The Canadian Intelligence Community—Control and Accountability-1996, Chapter 27," November 1996
[21] Annual Report of the Communications Security Establishment Commissioner, 1996-1997 Available on-line at: www.ocsec-bccst.gc.ca/ann-rpt/1996-97/index_e.php
[22] Frost, Spyworld, pp. 240-42
[23] Annual Report of the CSE Commissioner, 1997-98. Available online at: www.ocsec-bccst.gc.ca/ann-rpt/1997-98/index_e.php
[24] Annual Report of the CSE Commissioner, 1998-99. Available online at: www.ocsec-bccst.gc.ca/ann-rpt/1998-99/cover_e.php
[25] Annual Report of the CSE Commissioner, 1999-2000. Available online at: www.ocsec-bccst.gc.ca/ann-rpt/1999-2000/cover_e.php
[26] Annual Report of the CSE Commissioner, 2000-2001. Available online at: www.ocsec-bccst.gc.ca/ann-rpt/2000-2001/cover_e.php
[27] Bill C-36's formal title was "An Act to Amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering Act) and other Acts, and to enact Measures Respecting the Registration of Charities, in Order to Combat Terrorism." Its short title was the Anti-Terrorism Act. The portion of the omnibus Act referring to the CSE was contained at Part V.1, sections **273.61** to **273.7**

[28] I did call attention to some of these issues in a contemporaneous essay published during the debate over Bill C-36, Wesley Wark, "Intelligence Requirements and Anti-Terrorism Legislation," in Ronald J. Daniels, et al., The Security of Freedom: Essays on Canada's Anti-Terrorism Bill (Toronto: University of Toronto Press, 2001), pp. 287-96. See also my testimony regarding Bill C-36 to The House of Commons Standing Committee on Justice and Human Rights, Wednesday, October 24, 2001.
[29] CSE, "Backgrounder Documentation: Amendments to the National Defence Act/ Communications Security Establishment," October 2001. *Copy in the author's possession*.
[30] "Speaking Notes for the Honourable Art Eggleton, Minister of National Defence, for an Appearance before the Standing Committee of Justice, 23 October, 2001. *Copy in author's possession*.
[31] CSE's new statute is described, without critical commentary, in Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism," Intelligence and National Security, 22, no. 4 (August 2007), pp. 474-76.
[32] CSE Commissioner Annual Report, 2001-2002, tabled in Parliament on June 12, 2002. Available online at: www.ocsec-bccst.gc.ca/ann-rpt/2001-2002/cover_e.php
[33] ibid., p. 12
[34] Communications Security Establishment Commissioner, Annual Report 2002-2003, June 2003. Available on-line at: www.ocsec-bccst.gc.ca/ann-rpt/2002-2003/cover_e.php
[35] Communications Security Establishment Commissioner, Annual Report 2003-2004, June 2004. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2003-2004/cover_e.php
[36] Communications Security Establishment Commissioner, Annual Report 2004-2005, April 2005. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2004-2005/cover_e.php
[37] Communications Security Establishment Commissioner, Annual Report 2005-2006, April 2006, available online at: www.ocsec-bccst.gc.ca/ann-rpt/2005-2006/cover_e.php
[38] The story was first reported in a front page story in the New York Times by James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers without Courts," The New York Times, December 16, 2005. A fuller treatment of NSA eavesdropping on US communications was published subsequently by Risen in his book, State of War: The Secret History of the CIA and the Bush Administration (NY: Free Press, 2006), chapter 2.
[39] Communications Security Establishment Commissioner, Annual Report, 2005-2006, April 2006, online at www.ocsec-bccst.gc.ca/ann-rpt/2005-2006/cover_e.php
[40] Final Report of the House of Commons Standing Committee on Public Safety and National Security, Subcommittee on the Review of the Anti-Terrorism Act, "Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues," Chapter Seven: "Communications Security Establishment and the CSE Commissioner, March 2007
[41] Senate Special Committee on the Anti-Terrorism Act, "Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-Terrorism Act," February 2007, pp. 77-79
[42] Submission of the Office of the Privacy Commissioner to the Senate Special Committee on the Anti-Terrorism Act, May 9, 2005.

[43] Communications Security Establishment Commissioner, Annual Report, 2006-2007. Tabled in the House on June 12, 2007. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2006-2007/cover_e.php
[44] ibid.
[45] ibid.
[46] Communications Security Establishment Commissioner, Annual Report, 2007-2008, May 2008. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2007-2008/cover_e.php
[47] ibid.
[48] Communications Security Establishment Commissioner, Annual Report, 2008-2009. June 2009. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2008-2009/cover_e.php
[49] ibid.
[50] Communications Security Establishment Commissioner, Annual Report 2009-2010, June 2010. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2009-2010/cover_e.php
[51] Communications Security Establishment Commissioner, Annual Report 2010-2011, June 2011. Available online at www.ocsec-bccst.gc.ca/ann-rpt/2010-2011/cover_e.php
[52] ibid.
[53] For some commentary on data mining as a national security practice see: Oscar Gandy, "Data Mining, Surveillance and Discrimination in the post 9/11 Environment," in Kevin Haggerty and Richard Ericson, eds., The New Politics of Surveillance and Visibility (Toronto University of Toronto Press, 2006), 363-84; Ira S. Rubenstein et al., "Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches," The University of Chicago Law Review, 75, no. 1 (2008), 261-85; Christopher Slobogin, "Data Mining and the Security-Liberty Debate," University of Chicago Law Review, 75, no. 1 (2008), 343-62; Reg Whitaker, "A Faustian Bargain? America and the Dream of Total Information Awareness," in Haggerty and Ericson, eds., The New Politics of Surveillance and Visibility (2006), 141-70.
[54] Communications Security Establishment Commissioner, Annual Report, 2006-2007, "Reviews currently underway that I will be reporting on in the next fiscal year include examinations of CSE's activities related to counter-terrorism, its use of metadata…" Available online at www.ocsec-bccst.gc.ca/ann-rpt/2006-2007/cover_e.php
[55] The CSE website houses some descriptive pages on the Tutte Institute. See http://www.cse-cst.gc.ca/utte/index-eng.html
[56] See for example, the recent issue of Foreign Policy magazine, with articles by Thomas Rid, "Think Again: Cyberwar," and the rebuttal by John Arquila, "Cyberwar is Upon Us," Foreign Policy, March/April 2012, pp. 80-85; Richard Clarke, Cyber War: The Next Threat to National Security and What to do About It (New York: Harper Collins, 2010)
[57] "Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada," available online at www.publicsafety.gc.ca/prg/ns/cbr/ccss-scc-eng.aspx
[58] Private communication.
[59] Statement by the Prime Minister of Canada on the Shared Vision for Perimeter Security and Economic Competitiveness between Canada and the United States," February 4, 2011. http://www.pm.gc.ca
[60] Wesley K. Wark, "Smart Trumps Security: Canada's Border Security Policy since 11 September," in Daniel Drache, ed., Big Picture Realities: Canada and Mexico at the Crossroads (Waterloo, Ontario: Wilfrid Laurier University Press, 2008), pp. 139-152

[61] "The Canada-US Smart Border Declaration: Building a Smart Border for the 21st century on the Foundation of a North American Zone of Confidence," December 12, 2001. Available on-line at http://www.dfait-maeci.gc.ca/anti-terrorism/declaration-en.asp; Reg Whitaker, "Securing the 'Ontario-Vermont Border': Myths and Realities in post-9/11 Canadian-American Security Relations," International Journal, 60 (Winter 2004-2005), pp. 53-70

[62] "The Canada-U.S. Smart Border Declaration: Action Plan for Creating a Secure and Smart Border," 2002. Available on-line at http://www.drait-maeci.gc.ca/anti-terrorism/actionplan-en.asp

[63] See the discussion in Wesley Wark, "The Search for an Intelligent Border: A Canadian Perspective," Woodrow Wilson International Center for Scholars, One Issue: Two Voices, Issue 13, October 2010, pp. 11-18;

[64] Government of Canada, Privy Council Office, "Securing an Open Society: Canada's National Security Policy," April 2004.

[65] On the Security and Prosperity Partnership see the discussion in Wark, "Smart Trumps Security;" Council on Foreign Relations, "Building a North American Community: Report of the Independent Task Force," May 2005; Danielle Goldfarb, "The Canada-Mexico Conundrum: Finding Common Ground," C.D. Howe Institute, Toronto, Border Papers, no. 91, July 2005

[66] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar [O'Connor Commission], 2006, Report of the Events Relating to Maher Arar: Analysis and Recommendations, chapter 9, recommendation 6, p. 331

[67] ibid.

[68] Thomas D'Aquino and Michael Hart, "A New Start at Fixing U.S.-Canada Border," The Financial Post, February 9, 2011.

[69] Roland Paris, "Canada-US Perimeter Plan: From Aspiration to Action," December 8, 2011. Online at the Centre for International Policy Studies blog, http://cips.uottawa.ca

[70] Government of Canada, Perimeter Security and Economic Competitiveness Action Plan, "Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness," December 2011. Available online at www.borderactionplan.gc.ca

[71] ibid., p. 4

[72] ibid.

[73] ibid., p. 25

[74] ibid., p. 28

[75] The Office of the Privacy Commissioner submitted a report, "Fundamental Privacy Rights within a Shared Vision for Perimeter Security and Economic Competitiveness" to the Border Working Group that was established to hear public representations following the February 2011 leaders declaration

[76] Perimeter Security and Economic Competitiveness Action Plan, p. 32

[77] House of Commons of Canada, First Session, 41st Parliament, Bill C-30, "An Act to Enact the Investigating and Preventing Criminal Electronic Communications Act," First Reading, February 14, 2012. See also the helpful Legislative Summary prepared by the Library of Parliament, Publication No. 41-1-C30-E. 15 February, 2012.

[78] Minister of Public Safety Vic Toews briefly details the previous legislative history in an Op Ed printed in the National Post on February 24, 2012. As he notes, draft

legislation, (following lengthy prior study and public consultations dating back to 1999), was introduced by the Liberals in 2005; private members bill were introduced in 2007 and 2009 and the Conservatives twice tried to enact legislation in 2009 and 2010. Vic Toews, "Shedding Light on Bill C-30."

[79] For a detailed analysis of the significance of access to Basic Subscriber Information sought by the legislation, see the document by Christopher Parsons (a Ph.D. candidate in Political Science at the University of Victoria), "The Issues Surrounding Subscriber Information in Bill C-30," February 28, 2010, available at Parson's blog at www.christopher-parsons.com

[80] Michael Geist kindly shared with me the results of an ATIP request to the RCMP that is a snapshot of RCMP Basic Subscriber information requested from TSPs in (fiscal) 2010. The voluntary provision rate from TSP's was 93.6% on a high volume of 28, 143 requests. See also Michael Geist, "Why Governments Can't Pass a Privacy Bill," Ottawa Citizen, February 21, 2012, at p. D2

[81] This concept of 'discipline' is closer to a notion of 'professionalism' and is not to be confused with the now- classic analysis of discipline as a mode of surveillance discussed in Michel Foucault's, Discipline and Punish: The Birth of the Prison (NY: Random House, 1975)

[82] For a succinct expression of the concerns of the Privacy Commissioner of Canada, see Jennifer Stoddart's Open Letter to Minister Vic Toews, posted online as "Lawful Access Legislation May Threaten Our Rights and Freedoms," 27 October, 2011, available online at www.huffingtonpost.ca/jennifer-stoddart/lawful-access-legislation_b_1035386.html

[83] For a contrary view see Philippa Lawson, "Moving Towards a Surveillance Society," BC Civil Liberties Association, online at www.bccla.org

[84] Bea Vongduoangchanh, "Conservatives' Controversial Internet Surveillance Bill C-30 Culd be 'A long Time in Purgatory,'"The Hill Times, March 2, 2012

[85] For other cogent suggestions on how to make Bill C-30 more workable, see Michael Geist, "Why a Lawful Access Compromise Can be Found," February 15, 2012, available on the archived section of Professor Geist's blog at www.michaelgeist.ca