Communications Security Establishment Canada (CSEC), Structures of Secrecy, and Ministerial Authorization after September 11*

Kevin Walby,
and Seantel Anaïs

Introduction

The Communications Security Establishment Canada (CSEC) is Canada's foreign signals intelligence (SIGNIT) agency. Its closest counterparts are the National Security Agency (NSA) in the United States, the British Government Communications Headquarters (GCHQ) in the United Kingdom, the Government Communications Security Bureau (GCSB) in New Zealand, and the Defence Signals Directorate (DSD) in Australia. CSEC's mandate is to encrypt government communications and collect foreign signals intelligence. Its covert interception technologies that search voice and keyword patterns capture information transmitted through radio, Internet, satellite, and microwave towers,[1] supporting Canadian intelligence and security capabilities related to "communications surveillance." Headquartered in urban Ottawa, CSEC has a number of permanent SIGNIT stations, including near Leitrim, Ontario; Alert, Nunavut; Gander, Newfoundland; and Masset, British Columbia. In 2008, the federal government announced that it would spend at least $880 million to build a new Ottawa facility. CSEC also has mobile intercept stations that could be almost anywhere, at any time.

CSEC staff are trained in languages, encryption, decoding, engineering, and information technology. The secretive nature of CSEC means that—as an organization—it is subject to limited accountability measures. CSEC is reviewed by the Office of the Communications Security Establishment Commissioner (OCSEC), an arms-length agency that was created in 1996, although questions have been raised about what authority this commissioner has. Little is known about CSEC, and few accounts of their practices have been disclosed, despite the role of intelligence in controversies that stem from post-9/11 security certificate and rendition cases. Nearly 20 years ago,

* We thank Jeffrey Monaghan and the reviewers for their comments.

1 Jean-Paul Brodeur, "The Globalization of Security and Intelligence Agencies: A Report on the Canadian Intelligence Community," in *Democracy, Law, and Security: Internal Security Services in Contemporary Europe*, ed. Jean-Paul Brodeur, Peter Gill, and Dennis Tollborg (Aldershot: Ashgate Publishing, 2003).

Canadian Journal of Law and Society / Revue Canadienne Droit et Société, 2012, Volume 27, no. 3, pp. 363–380.

ex-CSEC employee Mike Frost said he was asked (by the NSA) to conduct surveillance that exceeded the CSEC mandate. He suggested that CSEC engaged in economic and immigration intelligence gathering and in monitoring Québec separatists.[2] However, Frost's work only refers to the 1980s. This article assesses how recent extensions of CSEC powers contribute to Canada's surveillance and intelligence legacies stemming from the events of September 11, 2001.

Both CSEC and Canada's domestic HUMINT spy service, the Canadian Security Intelligence Service (CSIS), received budgetary increases after September 2001.[3] CSEC's budget has been expanded from $45 million in the late 1990s to nearly $400 million by 2012, reflecting an increased concern with security intelligence in Canada. CSEC's workforce has doubled from 900 employees in the late 1990s to more than 2,000 by 2012. Much of their work since September 2001 has extended to intelligence supporting the occupation in Afghanistan, where CSEC intercepts the communications of "combatants" and provides SIGNIT for Canadian troops. Scholars are slowly learning just how extensively CSEC was involved in producing intelligence leading to the security certificate detentions and secret trials in Canada. It has also been noted that CSEC provided intelligence for detection of the so-called Toronto 18[4] and a smaller group of Muslim men in an Ottawa-based operation referred to as "Project Samosa," which also involved the Royal Canadian Mounted Police (RCMP). CSEC thus conducts military-related surveillance, as well as national security and police-related surveillance, yet little is known about how CSEC practices intersect with law.

Since the Canadian Anti-Terrorism Act was passed in 2001, the CSEC mandate has expanded to include interceptions of communications involving foreign bodies that begin or end in Canada. Their interception of private communications is sanctioned through Ministerial Authorization. Such surveillance does not require prior judicial authorization, and Ministerial Authorizations are only reviewed by the OCSEC after the fact. The legislative change appears in section 273.65(1) of the National Defence Act (NDA). In principle, CSEC's pursuit of its intelligence priorities is governed by rules that vary depending on whether or not intelligence intercepts are collected to facilitate the work of CSIS or the RCMP. When CSEC acts outside of its role as a technical arm of CSIS or the RCMP, it has its own legal powers to conduct intercepts—the rules vary depending on whether or not interceptions have a Canadian nexus. Foreign intelligence intercepts without a Canadian nexus are not subject to any statutorily mandated oversight.[5] In cases under

---

2 Mike Frost and Michel Gratton, *Spyworld: How CSE Spies on Canadians and the World* (Toronto: Seal Books, 1995).

3 See generally Colleen Bell, "Surveillance Strategies and Populations at Risk: Biopolitical Governance in Canada's National Security Policy," *Security Dialogue* 37, 2 (2006).

4 Martin Rudner, "Canada's Communications Security Establishment, Signals Intelligence and Counter-Terrorism," *Intelligence and National Security* 22, 4 (2007), 482.

5 Antonio Lamer, *Communications Security Establishment Commissioner Annual Report, 2003-2004* (Ottawa: Minister of Public Works and Government Services Canada, 2004).

Ministerial Authorization where a foreign signal originates in or is sent to Canada, CSEC is generally not subject to the constraints of "lawful access" outlined in the *Criminal Code* and the NDA.

Reviews of CSEC's Ministerial Authorizations do not occur until after the authorization has closed. Even then, the OCSEC only have limited information and cannot share their findings. It is old news that CSEC is not subject to judicial review and that their practices are not based on evidentiary standards. New is the veneer of legality that Ministerial Authorization provides to warrantless surveillance. Because section 273.64(2) of the NDA prohibits intelligence intercepts "directed at Canadians or any person in Canada," Ministerial Authorization is configured as a system of legal exception that grants CSEC the authority to intercept private communications in pursuit of foreign intelligence. CSEC intercepts of private communications with a Canadian nexus may be authorized by the Minister of National Defence if he/she is satisfied that the "expected foreign intelligence value of the information that would be derived from the interception justifies it."[6] But it is difficult to know if that standard is met, or how wide the net is cast.

Socio-legal scholars have not focused on CSEC. Perhaps it is assumed that CSEC does not have much to do with law, since intelligence is traditionally conceptualized as outside the principles and procedures of due process. Yet law crosscuts intelligence work in numerous ways.[7] Tellingly, CSEC's own public literature defines Ministerial Authorization as a "legal shield," and former CSE Commissioner Antonio Lamer has called Ministerial Authorization a "strange sort of creature" as far as legal standards go.[8] In this article, we address questions pertaining to the legal standing of Ministerial Authorization and its role in CSEC practices. We explore just what kind of legal mechanism Ministerial Authorization is and what it reveals about the relationship between Canadian law and intelligence activities. First we examine literature on CSEC with a focus on security intelligence and law. Then we analyze newspaper articles, OCSEC reports, and the results of access to information requests to reflect on the intelligence practices of CSEC. We use Ericson's concept of counter-law to focus our inquiry into the Ministerial Authorizations that enable CSEC interceptions of private communications.[9] Finally, we assess what Ministerial Authorization means for the structure and extension of state secrecy.

---

6 *National Defence Act*, RSC 1985, c N-5, s 273.68.

7 See, e.g., Stephane Lefebvre, "Canada's Legal Framework for Intelligence," *International Journal of Intelligence and Counterintelligence* 23, 2 (2010), 247–95; Steven Penney, "National Security Surveillance in an Age of Terror: Statutory Powers & *Charter* Limits," *Osgoode Hall Law Journal* 48, 2 (2010), 247–86; Brodeur, "The Globalization of Security and Intelligence Agencies," 210–64; and see also Peter Gill, *Policing Politics: Security Intelligence and the Liberal Democratic State* (London: Routledge, 1994).

8 Antonio Lamer, *Communications Security Establishment Commissioner Annual Report, 2004–2005* (Ottawa: Minister of Public Works and Government Services Canada, 2005), 8.

9 Richard Ericson, *Crime in an Insecure World* (London: Polity, 2007).

CSEC, Security Intelligence, and Law

CSEC was established in 1946 after Canada was drawn into collecting SIGNIT with the United Kingdom, the United States, Australia, and New Zealand during World War II. This alliance was referred to as the British–US Agreement and was signed in March 1946. At that time, CSEC was called the Communications Branch of the National Research Council.[10] In 1975, the agency was renamed CSEC and placed under the administrative control of the Department of National Defence (DND)—it was transferred from the National Research Council to DND after the Canadian Broadcasting Corporation revealed the existence of the agency. SIGNIT at this time focused on Cold War consulate spying and interception of trade secrets. The CSEC worked closely with the NSA in the United States. CSEC was (and still is) involved in preventing wiretaps at Canadian consulates, preventing interceptions of communications on Parliament Hill, and encrypting government computer systems.

Before 2001, policy directives for CSEC were issued from the Privy Council Office and Prime Minister or set in-house. CSEC had no legal standing until December 18, 2001, when Bill C-36, known as the Anti-Terrorism Act, gained assent.[11] The statutory basis of CSEC comprises three elements: the collection and analysis of foreign intelligence, guidance related to governmental information security, and technical and operational support for federal security and law enforcement organizations. Part V.1 of Bill C-36 authorizes CSEC to collect information pertaining to foreign entities even when those targets involve other persons in Canada. Bill C-36 and section 273.65 of the NDA empower the Minister of Defence to play a role in selecting entities to target with CSEC intercepts. Ministerial Authorizations are prepared and reviewed by in-house lawyers at the Department of Justice. There have been nearly 30 since 2002. Section 273.62 of the NDA also gives the Chief of CSEC new powers to manage and control all matters related to the organization. Before 2011, the National Security Advisor in the Privy Council Office (PCO) commented on policy issues pertaining to CSEC and communicated intelligence to the Prime Minister. However, on November 16, 2011, CSEC became an independent unit in the DND portfolio, reporting only to the DND Minister.

Intelligence agencies do not have evidentiary standards for producing information. Instead, they pick up whatever they can wherever they can.[12]

---

10 See, e.g., Kurt Jensen, *Cautious Beginnings: Canadian Foreign Intelligence, 1939–1951* (Vancouver: University of British Columbia Press, 2008); Wesley Wark, "Learning to Live with Intelligence," *Intelligence and National Security* 18, 4 (2003), 1–14; Martin Rudner, "Canada's Communications Security Establishment from Cold War to Globalization," *Intelligence and National Security* 16, 1 (2001), 97–128.

11 Jean-Paul Brodeur and Stephane Leman-Langlois, "Surveillance Fiction or Higher Policing?" in *The New Politics of Visibility and Surveillance*, ed. Kevin Haggerty and Richard V. Ericson (Toronto: University of Toronto Press, 2006).

12 Vesting authority in CSEC officials is of potential concern given the differences that Roach notes between evidence in criminal law enforcement and information in intelligence as well as the blurring of evidence and intelligence post-9/11. Evidence pertains to past events,

While there are major differences between evidence in criminal law and information in intelligence, CSEC operations are limited by specified protocol in the NDA. According to the NDA, CSEC intelligence work must focus on foreign-related entities and signals, the information should have a value that justifies its collection, the privacy of Canadians should be protected, and collection of information should pertain to international affairs, defence, or security. The CSE Commissioner (see section 273.63 of the NDA) has sworn that CSEC capabilities are not used to spy on Canadians and its activities are conducted within the parameters of law. But there have been counter-claims. In 1994, for instance, former CSEC employee Mike Frost published a book on his work with CSEC, in which he says he spied on Canadians.[13] Other former employees also came forward with stories about spying on foreign diplomats. Because of these claims concerning CSEC's accountability, the OCSEC was established in 1996. The CSE Commissioner is expected to receive complaints about CSEC's lawfulness and ensure that the agency acts legally. However, outside what appears in OCSEC reports, little is known about the agency because the Security of Information Act (which replaced the Official Secrets Act) and other legislation are used to keep employees duty-bound to secrecy. CSEC is basically exempt from the Access to Information Act, and OCSEC reports show that complaints are always deemed unworthy of investigation or found not to have merit.[14]

Oversight is problematic in security intelligence for numerous reasons. CSIS, for instance, is subject to the Security Intelligence Review Committee (SIRC), which was created under the CSIS Act to oversee their intelligence activities. The Prime Minister and Privy Councilors appoint members of SIRC. SIRC produces reports, allowing some information about the practices of CSIS to become a matter of the public record. Yet many of the SIRC reports are protected through classification and never revealed. Moreover, the existence of SIRC does not result in transparency and accountability within CSIS,[15] nor has it prevented renditions to torture and secret trials. Many people have called for parallel oversight of CSEC,[16] yet CSEC's structure of

---

while intelligence is collected on the basis of perceived future threats. Evidence becomes a matter of the public record, while intelligence remains an official secret. The other concern here is that in the post-9/11 context, where intelligence-led policing has become the norm, pre-emptive intelligence might be changing policing, too. See, e.g., Kent Roach, "The Eroding Distinction Between Intelligence and Evidence in Terrorism Investigations," in *Counter-Terrorism and Beyond*, ed. N. McGarrity, A. Lynch, and G. Williams (Abington: Routledge, 2010), 48–68; Christopher Murphy, " 'Securitizing' Canadian Policing: A New Policing Paradigm for the Post 9/11 Security State?" *Canadian Journal of Sociology* 32, 4 (2007), 449–75; Brodeur, "The Globalization of Security and Intelligence Agencies," 210–64.

13 See generally Frost and Gratton, *Spyworld*.

14 See Craig Forcese, "Canada's National Security 'Complex': Assessing the Secrecy Rules," *IRPP Choices* 15, 5 (2009).

15 See Geoffrey Weller, "Assessing Canadian Intelligence Literature: 1980–2000," *International Journal of Intelligence and Counterintelligence* 14, 1 (2001).

16 See Roy Rempel, "Canada's Parliamentary Oversight of Security and Intelligence," *International Journal of Intelligence and Counterintelligence* 17, 4 (2004).

secrecy is not simply a matter of domestic law. Many of the exemptions pertain to international intelligence agreements enacted in the Cold War era.[17] Any information obtained in confidence of a foreign state will remain an official secret under these agreements. The combination of these international intelligence agreements with domestic law, such as the Security of Information Act, means there is little recourse through access to information legislation—this is pertinent to the idea of structures of secrecy that we return to later in this article.

Our interest is in CSEC practices since the Anti-Terrorism Act was passed. CSEC has been transformed as a result of its new funding and the broader security intelligence efforts going on under the auspices of the global "War on Terror." This transformation of CSEC represents one surveillance legacy of September 2001. Next, we explore how CSEC practices intersect with law.

CSEC Before and After September 11, 2001

We have collected all newspaper materials published regarding CSEC since the early 1980s, and we have analyzed these to understand the public image of CSEC. We have also consulted the annual reports of the OCSEC and submitted access to information requests in 2010 to other federal government agencies, such as CSIS, the RCMP, and DND, to locate memoranda of understanding (MOUs) between CSEC and these agencies. These MOUs were exempted and redacted using section 15(1) and 16(2)(c) of the Access to Information Act. Section 15(1) of the Access to Information Act refers to information that could be injurious to international affairs, the defence of Canada, or to the "detection, prevention or suppression of subversive or hostile activities." Section 16(2)(c) of the Access to Information Act refers to information regarding the vulnerability of particular buildings or systems, including computer and communication systems. While these MOUs provide a glimpse into the practices of CSEC and their intersection with law, one finding is that CSEC is nearly impossible to research using traditional (e.g., evaluation of open source material) and less-traditional (e.g., access to information requests) methodological strategies. Despite the barriers, an analysis of these data starts to illustrate the connection between Ministerial Authorization, CSEC intelligence, and the structure of state secrecy.

The public face of CSEC

An analysis of daily newspaper articles that mention CSEC reveals that the issue of terrorism does not dominate public discussion of CSEC before 2001. In 1984, Solicitor-General Robert Kaplan testified that CSEC had the capability to monitor domestic and international communications, which was one of the first indications by a government official that CSEC existed

[17] See Ian Leigh, "Legal Access to Security Files: the Canadian Experience," *Intelligence and National Security* 12, 2 (1997).

and could intercept the communications of Canadians. Also in 1984, when new legislation was passed resulting in the creation of CSIS, former Solicitor-General Allan Lawrence noted that the change did nothing to address the lack of transparency and accountability in CSEC. Prime Minister Jean Chrétien did not say much in 1994 about the growing public awareness of CSEC, although the media hounded him after Mike Frost's revealing publication of *Spyworld*. In 1995, a series of articles appeared about former CSEC employee Jane Shorten, who was fired some years earlier; she claimed that CSEC was spying on nations such as Japan and Mexico.[18] The Auditor-General critiqued the management of CSEC and CSIS in 1996, arguing that the agencies suffered from ballooning budgets and little oversight.[19]

Since September 2001, CSEC has focused primarily on terrorism, as has the media coverage. CSEC immediately entered into close collaboration with the NSA after September 11. In late October of 2001, CSEC told the Commons Defence Committee that they needed more funding in addition to the $37 million announced earlier that month. Later in 2001, CSE Commissioner Claude Bisson argued that the new powers granted to CSEC under anti-terrorism law could lead to invasions of privacy. Wesley Wark from the University of Toronto commented in 2002 on the limitations of CSEC compared to intelligence agencies in other countries and on the need for organizational growth.[20] Over the next six years, CSEC did grow, receiving an additional $280 million to be spent between 2002 and 2008. The anti-terrorism legislation and the revision of the Official Secrets Act to create the Security of Information Act also resulted in the reclassifying of government protocol, making more government employees permanently bound to secrecy. In addition, CSEC placed recruitment ads in eight Canadian newspapers,[21] a rare move for the clandestine agency.

In 2004, Auditor-General Sheila Fraser commented on intelligence agencies in Canada, including CSEC.[22] She noted an increasingly close connection between the RCMP and CSEC, the dearth of information provided in the CSE Commissioner's reports, the lack of oversight, and the fact that the Commissioner can only review a fraction of CSEC's activities. In 2006, there were news stories on CSEC suggesting that the NSA had been tracking phone calls of citizens since September 11, 2001. Then Chief of CSEC John Adams responded to inquiries from then CSE Commissioner Antonio Lamer, a former Supreme Court justice. Lamer's inquiries pertained to the practices of CSEC and whether they abided by Canadian laws. Also in 2006, members of the *National Post* were allowed a guided tour of a CSEC

---

18 Greg Weston, "They Spy with Their Little Eyes, Even Though They Say They Aren't," *Ottawa Citizen* (November 15, 1995), A2.

19 "Auditing the Spies," *Ottawa Citizen* (November 27, 1996), A14.

20 Wesley Wark, "We Must Review CSE's Performance, Not Legality," *Globe and Mail* (July 29, 2002), A15.

21 Kathryn May and Jim Bronskill, "Secretive Communications Security Establishment goes Public with Massive Recruitment Drive," *The Gazette* [Montreal] (May 13, 2002), A13.

22 T. Walkom, "Who Oversees our Spies?" *Toronto Star* (February 14, 2004), F03.

facility, though this was reported to be highly scripted.[23] As reported in news coverage regarding the CSE Commissioner in 2007, the OCSEC report that year specified that it was difficult to know if the practices of CSEC were in accord with laws that the agency is subject to, even for the Commissioner. In 2010, CSEC was mentioned in the context of foiling an alleged terror plot in Ottawa, Canada. The suspects were using public computers at an Ottawa library to communicate about their plans. CSEC computer "sniffers" or filters detected the discussions by using keyword combination searches.[24] The information was relayed to CSIS and the RCMP, the latter of which launched a surveillance mission called "Project Samosa" to build evidence. In July 2012, there was coverage of CSEC's decision to stop publishing its annual plans and priorities bulletin.[25] Then in August of 2012, CSEC was mentioned in the context of RCMP surveillance of anti-pipeline environmental groups.[26]

CSEC undeniably has a public face, albeit a tightly managed one. After September 2001, the public face of CSEC was linked to anti-terrorism. Intelligence agencies are part of day-to-day administration in government,[27] but the actual intelligence practices of CSEC remain a secret for the public and for most civil servants. Moreover, Ministerial Authorization has not been discussed in newspaper representations of CSEC.

The OCSEC and official discourse

Until December 2001, the CSE Commissioner carried out duties under the authority of Orders in Council. As of April 2007, the provision of administrative activities and budget was no longer tied to the Privy Council Office and was moved to DND. In April 2009, the OCSEC was granted its own parliamentary appropriation; its budget became independent from DND's. Claude Bisson was commissioner from 1996 to 2003; Antonio Lamer was commissioner from 2003 to 2006; Charles Gonthier was commissioner from 2006 to 2009; and Robert Décary is the current commissioner. The OCSEC releases annual reports based on the work of investigators. We examined these reports to understand how they frame CSEC work in three different periods: in the five fiscal years before September 11, 2001; in the six years following the passage of the Anti-Terrorism Act in 2001; and between 2008 and 2012, during which time Ministerial Authorization has been a central topic in OCSEC reports.

The early reports of the CSE Commissioner are somewhat defensive in tone. In July 1996, then Privacy Commissioner Bruce Phillips issued a

---

23 Stewart Bell, "Listening in on the Enemy: Canada's Master Eavesdroppers," *National Post* (April 15, 2006), A1.

24 Ian Macleod, Andrew Seymour, and Meghan Hurley, "Parliament Hill Alleged Terror Goal," *National Post* (August 28, 2010), A4.

25 Jim Bronskill, "Canada's Eavesdropping Agency Gets a little Quieter," *Vancouver Sun* (July 26, 2012), B2.

26 Michael Gottschalk, "Police identify 'Anonymous' Threat," *Montreal Gazette* (August 28, 2012), B13.

27 See Philip Davies, "Intelligence and the Machinery of Government: Conceptualizing the Intelligence Community," *Public Policy and Administration* 25, 1 (2010).

report to the Chief of CSEC that raised questions about whether CSEC was complying with privacy law or was eavesdropping on the political activities of Canadians. The CSE Commissioner responded in his report that CSEC employees undergo rigorous privacy training and that he was "satisfied that CSE has not targeted Canadian citizens or permanent residents." The CSE Commissioner also claimed that "CSE does not target Québec communications, or the Québec sovereignty movement,"[28] contrary to what former CSEC employees were claiming. In November 1996, the Auditor-General of Canada tabled a report called *The Canadian Intelligence Community*, finding that the CSEC lacked sufficient oversight. Yet the CSE Commissioner reports for 1997–1998 through 1999–2000 claim that CSEC was not breaking any laws and affirm the legality of CSEC's intelligence practices. In the report for 1998–1999, the Commissioner indicated that the "CSE has policies and practices to address the safeguarding and proper handling of inadvertently collected Canadian communications in accordance with the laws of Canada."[29] The Commissioner report in 1999–2000 similarly notes that there were no findings of "unlawful activity."[30]

However, each of these OCSEC reports also highlight the legal vulnerabilities associated with CSEC activities. For instance, the CSE Commissioner report for 1998–1999 addresses the issue of whether CSEC should be subject to the same oversight as CSIS. He argues that—unlike CSIS/RCMP—CSEC should not have to "maintain constant contact with the citizens of the nation," affirming that the intelligence gathering of CSEC should remain secret.[31] The Commissioner also describes what is called Law Day in CSEC: "Shortly after the end of the 1998–99 fiscal year, CSE sponsored its first ever Law Day. The event coincided with other Law Day celebrations across the country held annually to mark the anniversary of Canada's Charter of Rights and Freedoms."[32] In the 1999–2000 report, the Commissioner notes that he "paid particular attention this year to examining not only *what* CSE collects and retains but *how* CSE's intelligence holdings are generated . . . CSE is employing appropriate measures to safeguard the privacy of Canadians" (emphasis in original).[33] Likewise, the CSE Commissioner report for 2000–2001 emphasizes that the "CSE does not use its partners to circumvent the laws of Canada, nor does it provide partners with communications they could not legally collect for themselves."[34]

---

28 Claude Bisson, *Communications Security Establishment Commissioner Annual Report, 1997–1998* (Ottawa: Minister of Public Works and Government Services Canada, 1998), n.p.

29 Claude Bisson, *Communications Security Establishment Commissioner Annual Report, 1998–1999* (Ottawa: Minister of Public Works and Government Services Canada, 1999), n.p.

30 Claude Bisson, *Communications Security Establishment Commissioner Annual Report, 1999–2000* (Ottawa: Minister of Public Works and Government Services Canada, 2000), 6.

31 Ibid., n.p.

32 Bisson, *CSEC Annual Report, 1998–1999*, n.p.

33 Bisson, *CSEC Annual Report, 1999–2000*, 3.

34 Ibid., 10.

The CSE Commissioner reports published between 2001–2002 and 2007–2008 adopt a different character, focusing on the new organization and statutory mandate of CSEC. The CSE Commissioner report for 2001–2002 contends that the Anti-Terrorism Act of 2001 and the revised NDA "introduced new elements to the roles of CSE and my Office" as well. The Commissioner writes that "Despite concerns expressed about the haste with which the legislation was drafted and debated . . . those parts of the legislation that deal with CSE and the CSE Commissioner benefited from years of discussion within government long before."[35] One complaint was received, but it was found to lack merit. As with the previous CSE Commissioner reports, no incidents of "unlawfulness or unauthorized activity" were identified between 2001 and 2008. Further, each report underscored the presence of measures to protect the privacy of Canadians in the retention and use of intercepted information.

During this period, the issue of Ministerial Authorization began to be noted in these reports, and in 2003–2004 the Commissioner wrote that "CSE has continued to improve the MA structure and strengthened the MA management and accountability mechanisms."[36] The Commissioner did highlight one item of concern: "a more general issue about the structure of and process for using ministerial authorizations did arise. Certain weaknesses in policies and procedures related to these activities were brought to CSE's attention."[37] In 2004–2005, the Commissioner commented on how Ministerial Authorizations are a "strange sort of creature" as far as legal standards with warrants and judges go.[38] The lack of need for a warrant is not strange in the field of intelligence; what is unusual is enshrining the ability to conduct warrantless communications surveillance in statutory law.

The CSE Commissioner reports from 2007–2008 to 2010–2011 problematize Ministerial Authorization while continuously confirming the legality of CSEC activities and underscoring the small relative proportion of unintentionally intercepted private communications.[39] In the 2007–2008 report, the Commissioner did find that expectations for Ministerial Authorizations had not been met, but he failed to elaborate on the implications. The Commissioner also commented on how lack of information made it difficult for him to prepare proper reports, impairing his ability to determine whether CSEC acts in accord with the law. The CSE Commissioner report for 2008–2009 reflected on the findings of the Auditor-General of Canada, which noted the ambiguities in the laws that CSEC is subject to and the challenge of the CSE Commissioner to hold the CSEC to account. This report suggests that

[35] Claude Bisson, *Communications Security Establishment Commissioner Annual Report, 2001–2002* (Ottawa: Minister of Public Works and Government Services Canada, 2002), 2–3.

[36] Lamer, *CSEC Annual Report, 2003–2004*, 7.

[37] Ibid., 9.

[38] Antonio Lamer, *Communications Security Establishment Commissioner Annual Report, 2004–2005* (Ottawa: Minister of Public Works and Government Services Canada, 2005), 8.

[39] See Robert Décary, *Communications Security Establishment Commissioner Annual Report, 2009–2010* (Ottawa: Minister of Public Works and Government Services Canada, 2010).

CSEC officials should record more information about their intelligence gathering to increase accountability, and it mentions that there were two Ministerial Authorizations for projects in Afghanistan the year prior. As Charters notes, more than half of the intelligence used by Canadian Forces in Afghanistan came from CSEC under such Authorizations.[40]

The commissioner reports raise questions about information management, accountability, and Ministerial Authorization. Although the commissioner has never found CSEC to be out of compliance (that they have reported), even post-9/11, the commissioners point to the legal quandary that is Ministerial Authorization. These reports raise the question of whether CSEC is in line with Canadian law, but can only provide cautious answers.[41]

CSEC and access to information

We have also examined disclosures through access to information procedures as a way of understanding the intelligence work of CSEC in the years following September 2001. A memorandum of understanding (MOU) establishes a relationship for the distribution of resources between two government agencies as it concerns their joint governance activities. While we obtained MOUs between CSEC and other government agencies spanning from 1994 to 2010, below we concentrate on MOUs established after September 2001. The ATI material we received is heavily redacted and exempted, but it begins to sketch the contours of the relationship between CSEC and other government agencies. Below we assess the new register of legal knowledges deployed in MOUs after 2001.

The first MOU post-2001 that we obtained is from 2003, and it is between CSEC and DND/Canadian Forces as it regards the authority to conduct military-related SIGNIT activities. The MOU refers to CSEC's new statutory mandate under the Anti-Terrorism Act "to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence to the Government of Canada."[42] The Canadian Forces Information Operations Group is enabled by this MOU to routinely conduct foreign intelligence activities on behalf of CSEC. Another MOU from 2003 specifies the supporting role that the Canadian Forces Information Operations Group will play for CSEC by providing foreign intelligence.

We recovered three MOUs from 2006. The first is between DND and CSEC and concerns financial management and responsibilities for capital acquisitions in support of the Canadian Cryptographic Modernization Program. This program is managed by CSEC and deals with encryption for

---

[40] See David Charters, "Canadian Military Intelligence in Afghanistan," *International Journal of Intelligence and CounterIntelligence* 25, 3 (2012).

[41] Another question is whether their practices are in line with international law and the laws of countries in which CSEC intercepts private communications.

[42] All Department of National Defence material cited in this section was produced through request #A-2009-01100.

all government agency communications—two of the projects mentioned are the Secure Voice Re-key Infrastructure Project 2004–2007 and the Classified Security Management Infrastructure Project 2006–2016. The second MOU is between DND and CSEC concerning the provision of SIGNIT support to deployed military forces. The document mentions a Ministerial Authorization from May 2004 directing CSEC to deliver SIGNIT to troops in Afghanistan. According to the document, the goal of the mission in Afghanistan is to "provide assistance and support for the establishment and development of a stable, reliable, and democratic regime."[43] The document also states that CSEC provides SIGNIT to protect the "safety and security of Canadians at home and abroad."[44] The remainder of the document specifies the guidelines that govern the provision of SIGNIT by CSEC to support troops but also CF SIGNIT operations in Afghanistan. The third MOU is between CSEC and DND's Canadian Forces Cryptographic Support Unit and addresses the Government of Canada's Electronic Key Management System (EKMS) Sustainment Contract, and intelligence sharing with the NSA.

MOUs from 2007 and 2009 provide an overview of the division of labour within CSEC, detailing the treatment of classified and protected information. The 2007 MOU between CSEC and DND details practices around the identification of vulnerabilities and risk mitigation in the information technology networks of the Government of Canada. It mentions a Ministerial Authorization that enables CSEC "to intercept private communications for the purpose of protecting the computers system or networks of the Government of Canada from mischief, unauthorized use or interference."[45] The 2009 MOU between CSEC and the Canadian Forces Information Operations Group reviews three postings in CSEC: the operational authority, the technical authority, and the security authority. The operational authority "develops standards, and ensures they are followed by all users of the [redacted] system."[46] The technical authority is the Chief Information Officer, who works to ensure that information management and exchange between CSEC and the Canadian Forces Information Operations Group is efficient. The security authority is in charge of corporate or in-house security for CSEC, including security provisions for classified processing and physical security. The next MOU from 2009 discusses the treatment of classified and protected information, specifying that all information access in CSEC (by employees) must be cleared by the Director of Threat and Vulnerability Analysis.

What this ATI material shows is that CSEC is fully integrated into the structure of the federal government. They work on encryption for all government agencies. They take the lead on security intelligence with other intelligence agencies in Canada, and they work in tandem with Canadian military

43 Ibid.
44 Ibid.
45 Ibid.
46 Ibid.

operations. In addition, they are in charge of managing information obtained in confidence from foreign governments and ensuring that information is not leaked or hacked. All of these practices should be counted among the surveillance and intelligence legacies of September 11. The question is how this secrecy is organized in the face of further integration with agencies that do not follow CSEC's "need-to-know" approach, and how the authorizations for private intercepts are conducted.

Secrecy, Ministerial Authorization, and Counter-Law

CSEC and the structure of secrecy

The information management practices of CSEC detailed in this article are relevant to socio-legal discussions of secrecy. David Pozen provides an analytical discussion of shallow and deep secrecy that we draw on.[47] Scholars in sociology, law, and political science have not paid much attention to the structure of government secrets, he suggests. Pozen argues that secrets have four components: (1) how many people know the secret, (2) what kinds of people know the secret, (3) how much information they know, and (4) when they know what they know. Shallow secrets are secrets about which others know they know little. Deep secrets are those of which there is no public awareness. We use this typology to conceptualize the structure of secrecy that characterizes CSEC practices.

The first element of secrecy is how many people know about it. The more people who find out about a secret, the shallower it becomes. CSEC information appears to be operating near the realm of deep secrets, insofar as few people outside of the Prime Minister, the Minister of Defence, and CSEC employees are aware of their practices past or present, internationally or domestically. The secrecy of sources and methods in CSEC means that it is difficult to know what CSEC does and whether their sources and methods are reliable. The practices of CSEC remain cloaked under an amalgam of domestic security law and international intelligence agreements that prevent disclosure of almost all information pertaining to the agency.

The second element of secrecy is what kinds of people know about it. There are many possible audiences of secrets, and the fact that journalists, politicians, and the general public receive no information about CSEC intelligence practices again suggests that CSEC is operating near the realm of deep secrets. The legal context is key here, insofar as CSEC employees are bound to secrecy as part of their job description due to the criminalization of disclosure under the Security of Information Act and the Canada Evidence Act.[48] CSEC employees are not run-of-the-mill civil servants, and the planned leaks that happen with other government agencies are much less of a possibility. In his rendering of CSEC, Frost writes of filling out "de-indoctrination" papers that obliged him not to share any information about the inner

[47] See generally David Pozen, "Deep Secrecy," *Stanford Law Review* 62, 2 (2010).
[48] See Forcese, "Canada's National Security 'Complex'."

workings of CSEC.[49] Tellingly, there have been no leaks or testimonials since 2001.

The third element of secrecy concerns how much information is known. Not only do people outside the CSEC chain of command have sparse information about the agency, but within the agency the activities are compartmentalized to a higher degree than in other government agencies, meaning that there is low awareness of what happens from unit to unit. Frost and Gratton observe that CSEC is "extremely compartmentalized in its operations."[50] CSEC is able to control how much information people inside and outside the agency know. There were two small difficulties in this regard, according to Frost. First, some support staff that the CSEC used for basic operations were members of the Public Service Alliance of Canada (PSAC), and these unionized employees did not have the same security outlook as CSEC. Second, consulate and embassy staff were believed to be untrustworthy.

The fourth element of secrecy is how disclosure is timed and when information becomes known. Information pertaining to CSEC past and present is managed to prevent disclosure and awareness. For example, historians have had trouble gaining access to information regarding intelligence, the Communications Branch of the National Research Council, and World War II. Brodeur likewise points out that the CSE Commissioner cannot review any previous CSEC activities (say, from the 1980s),[51] and all data being produced within CSEC are protected far into the future under various laws, including the Security of Information Act.

National security intelligence is always subject to stricter information management than information located elsewhere in government. However, what Pozen calls "the power to conceal the fact of one's concealment" is high in CSEC.[52] CSEC is operating in a realm of deep secrecy insofar as even workers within CSEC are not aware of the information that is being withheld, or how to get at it. This information roadblock is more intense for journalists, scholars, politicians, and the public. The other element of secrecy here is the public face for CSEC that has been created with the CSE Commissioner. This element of secrecy concerns the link between official discourse and secrets—the annual reports of the CSE Commissioner being a form of official discourse that creates a veil of transparency. At the same time, CSE Commissioners have expressed frustrations in their inability to comment on the actual surveillance practices of the agency and ambiguities in the laws governing it. This latter issue has to do in part with Ministerial Authorization.

Ministerial Authorization

Ministerial Authorization operates to provide direction for interception of private communications and to ensure CSEC information is not disclosed.

---

49 See Frost and Gratton, *Spyworld.*
50 Ibid., 227.
51 Brodeur, "The Globalization of Security and Intelligence Agencies," 210–64.
52 Pozen, "Deep Secrecy," 309.

Under Ministerial Authorization, reviews of CSEC work do not happen until after the authorization has ended. We are not suggesting that judicial review, where privacy invasions are assessed prior to, would make CSEC practices acceptable; we are, however, raising questions about the intersection of intelligence and law in Canada. If the structure of secrecy with CSEC has not changed, why enshrine it in statutory law? The shift of the structure of secrecy into the legal field of Ministerial Authorization may be meant to build legitimacy for CSEC at a time when they are highly active in the "War on Terror," and when they intercept more private communications in Canada than ever before. A more probable explanation is the one that CSEC itself offers. CSEC's own public literature defines Ministerial Authorization as a "legal shield" without which "independent, cutting-edge Canadian collection and protection programs" would be impossible.[53]

Ministerial Authorization heightens the discretionary power of Ministers of National Defence and their closest staff by vesting in them the authority to use their judgment to decide matters of justice, privacy, accountability, and transparency. Because Ministerial Authorization addresses the challenges posed by the matters of due process that traditionally limit the authority of intelligence agencies to intercept the private communications of Canadians at home and abroad, it constitutes one of the mechanisms by which state agencies contort law for their own purposes. We argue that CSEC—and Ministerial Authorization specifically—helps us to know more about the practical operations of what Ericson calls "counter-law." Ericson specifies two elements of counter-law. Counter-law I refers to enacting new laws and manipulating existing law. These enactments are carried out in such a way as to undermine traditional principles, standards, and procedures of law or prevent these standards from being applied.[54] Here, the traditional boundaries demarcating the limits of different forms of criminal, civil, and administrative law—and the principles and procedures governing each sphere—are increasingly eroded and blocked. Bound up with the mechanisms and calculations of counter-law I, counter-law II takes the form of an assemblage of surveillance mechanisms. These capabilities draw together existing and new surveillance networks, as in CSEC's continuing collaboration with NSA coupled with their new intelligence activities in Afghanistan and their interception of private communications with a Canadian nexus. Developments in surveillance and the extension of existing technologies are combined to eliminate even the semblance of traditional standards, principles, and procedures of due process, and to prevent such standards from coming into effect.

The National Defence Act specifies that the Minister may only authorize CSEC intercepts if "they are essential to international affairs, defence or security."[55] The question of whether this threshold is met has been raised by

---

[53] *CSE's Ministerial Authorization*, http://www.cse-cst.gc.ca/home-accueil/media/ma-am-eng.html.
[54] Ericson, *Crime in an Insecure World*, 24.
[55] *National Defence Act*, RSC 1985, c N-5, s 273.68(d).

at least one CSE Commissioner. In his 2005–2006 report, former CSE Commissioner Lamer noted that "supporting documentation provided by CSE as part of requests for the Minister's authorization address the underlying foreign intelligence requirements only in general terms."[56] This practice of excepting CSEC from due process standards raises constitutional issues, not least in the case of the Charter section 8 protections pertaining to searches and seizures.[57] However, the perceived urgency of the "War on Terror" is offered to justify infringements on the rights of individuals who may otherwise be protected by the Charter. Ministerial Authorization renders the legal protections of the Charter and the "lawful access" provisions of the *Criminal Code* and CSIS Act redundant. While the thresholds that must be met to authorize an intelligence intercept are similar to the grounds that must be satisfied in the CSIS Act, the fundamental difference is that the person authorizing the intelligence intercept is an executive official. Ministers of National Defence and their closest staff cannot by any definition be considered disinterested adjudicators of search and seizure requests.[58] Ministerial Authorization thus invests the Minister and their closest staff with the power to render unilateral decisions on the basis of information that remains unverifiable. Since 2001 and the intensification of the "War on Terror," the CSEC has operated within a field of secrecy secured by the creation of legal exceptions in the form of Ministerial Authority.

Counter-law has become the paradigmatic expression of state sovereignty, especially in light of the visible failures of government to preempt catastrophic consequences of breaches in security apparatuses. As a result, counter-law names an ironic set of processes by which threats to law generate official surveillance responses that further threaten the rule of law. CSEC thus operates in a space of liminality where the legal protections of "lawful access" set out in the *Criminal Code* and CSIS Act become almost irrelevant. The exceptional autonomy of CSEC—and the secrecy that shrouds its intelligence-gathering functions—ensures that neither foreign intelligence intercepts nor those with a Canadian nexus will be subject to any semblance of due process. Further, CSEC exemplifies the erosion of boundaries between civil and administrative law by articulating Ministerial Authority as the entitlement of an executive power above the criminal and administrative protections guaranteed to Canadians at home and abroad. Finally, CSE Commissioner reports continually mention that OCSEC cannot readily review CSEC Ministerial Authorizations for intelligence work related to Canadian Forces operations in Afghanistan. Ministerial Authorization thus provides a "legal shield" designed to obscure at least some of the conduct of Canadian troops in

---

56 Antonio Lamer, *Communications Security Establishment Commissioner Annual Report, 2005–2006* (Ottawa: Minister of Public Works and Government Services Canada, 2006), 10.

57 The Supreme Court of Canada ruling on Afghan detainees, which states that section 7 and section 8 do not apply to "non-Canadians," is relevant for understanding what Canadian agencies can do outside Canada.

58 Also see Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008).

Afghanistan from civilian, government, and criminal law based oversight. This post-9/11 shift to Ministerial Authorization operates as a mechanism not only for directing the communications surveillance undertaken by CSEC, but more crucially as a means of keeping knowledge of their surveillance practices from public record.

Coda: Slippery Slopes as Far as the Eye Can See

Intelligence agencies must be analyzed as part of the federal government since they are subject to law and public policy. Yet information about CSEC practices is not readily available. The lack of transparency has ramifications for social scientists who want to understand the security intelligence practices of CSEC. There has been a move to create a public face for CSEC and maintain legitimacy in the context of lack of accountability and transparency (i.e., the CSE Commissioner). But annual reports from the OCSEC are sanitized, and the classified materials are not even available to MPs who sit on committees pertaining to national defence. The work of CSEC is thus a deep secret since it remains unknown from unit to unit within CSEC, in other branches of government, and in the media.

The shift to vesting powers in Ministerial Authorization has not altered the deep secrecy around CSEC's security intelligence practices, and Ministerial Authorization allows CSEC to operate with what the agency refers to as a "legal shield." However, we have not gone as far as other scholars to suggest that better oversight and greater recourse to legal regulation would make CSEC practices acceptable. For instance, Penney contends that certain CSEC practices pertaining to interception of domestic communications most likely violate section 8 of the Charter and need to be brought in line with Canadian law.[59] From a social justice or critical security studies perspective, this "greater law" slope is as slippery as advocating for more security intelligence. The renditions to torture and failures of SIRC oversight demonstrate that this legal apparatus is implicated in these surveillance legacies, as much as it is something that keeps surveillance in check. Appeals to protecting privacy, prior judicial review, and investigative necessity do not mount sufficient critiques of the basic idea of security and political surveillance. Reaffirming liberal values and legal frameworks through calls for amendments does little to challenge the surveillance legacies stemming from September 11, 2001.

Abstract

Communications Security Establishment Canada (CSEC) produces foreign signals intelligence for Canada's Department of National Defence. Before Canada's Anti-Terrorism Act was passed in 2001, CSEC had no statutory basis. Canada's Anti-Terrorism Act and the revised National Defence Act extended CSEC powers, allowing

[59] See Penney, "National Security Surveillance in an Age of Terror"; also see Rempel, "Canada's Parliamentary Oversight of Security and Intelligence."

the agency to collect foreign intelligence for communications with a Canadian nexus, thus contributing to post-9/11 surveillance and security intelligence legacies. Yet little is known about CSEC practices or CSEC's involvement in the "War on Terror." In this article, we examine the transformation of CSEC. We contribute to debates about communications surveillance and anti-terrorism laws by analyzing the results of access to information requests pertaining to CSEC intelligence and the reports of the Office of the Communications Security Establishment Commissioner. Focusing on the Ministerial Authorizations that enable CSEC's interceptions of private communications, which we conceptualize using Ericson's notion of counter-law, we also add to literature on the structure of secrecy by assessing CSEC information management practices.

Keywords: intelligence, security, secrecy, Communications Security Establishment Canada (CSEC)

Résumé

Le Centre de la sécurité des télécommunications Canada (CSTC) collecte des renseignements électromagnétiques étrangers pour le Ministère de la défense nationale du Canada. Avant l'adoption de la Loi antiterroriste en 2001, le CSTC n'avait pas de fondement statuaire. La Loi antiterroriste canadienne ainsi que la loi révisée sur la Défense nationale conféraient des pouvoirs élargis au CSTC, permettant à l'agence de recueillir des renseignements étrangers sur les communications ayant un rapport canadien et contribuant ainsi à l'héritage de la surveillance et des renseignements de sécurité au lendemain des évènements du 11 septembre 2001. Cependant, nos connaissances des pratiques du CSTC ou de son implication dans « la guerre contre le terrorisme » sont encore limitées. Dans cet article, nous examinons la transformation du CSTC. Nous contribuons aux débats sur la surveillance des télécommunications et sur la législation anti-terroriste en analysant les réponses aux demandes d'accès à l'information relatives aux renseignements collectés par le CSTC ainsi que les rapports du Bureau du Commissionnaire du Centre de la sécurité des télécommunications. En se concentrant sur les autorisations ministérielles qui ont permis au CSTC d'intercepter des télécommunications personnelles, que nous conceptualisons à l'aide de la notion d'Ericson de « contre-droit », nous contribuons aussi aux études sur les structures du secret par l'analyse des pratiques de gestion de l'information du CSTC.

Mots clés: renseignement de sécurité, sécurité, secret, Centre de la sécurité des télécommunications Canada (CSTC)

Kevin Walby
Department of Sociology, University of Victoria
PO Box 3050 STN CSC
Victoria, BC V8W 3P5