“CANADIAN EYES ONLY”: TECHNO-SECURITIZATION, JUST SURVEILLANCE, AND THE COMMUNICATIONS SECURITY ESTABLISHMENT

A Thesis Submitted to the
College of Graduate and Postdoctoral Studies
In Partial Fulfillment of the Requirements
For the Degree of Masters of the Arts
In the Department of Political Studies
University of Saskatchewan
Saskatoon

By

Harrison Baile

PERMISSION TO USE

In presenting this thesis/dissertation in partial fulfillment of the requirements for a Postgraduate degree from the University of Saskatchewan, I agree that the Libraries of this University may make it freely available for inspection. I further agree that permission for copying of this thesis/dissertation in any manner, in whole or in part, for scholarly purposes may be granted by the professor or professors who supervised my thesis/dissertation work or, in their absence, by the Head of the Department or the Dean of the College in which my thesis work was done. It is understood that any copying or publication or use of this thesis/dissertation or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to the University of Saskatchewan in any scholarly use which may be made of any material in my thesis/dissertation.

Requests for permission to copy or to make other uses of materials in this thesis/dissertation in whole or part should be addressed to:

Head of the Department of Political Studies

9 Campus Drive

University of Saskatchewan

Saskatoon, Saskatchewan S7N 5A5 Canada

OR

Dean

College of Graduate and Postdoctoral Studies

University of Saskatchewan

116 Thorvaldson Building, 110 Science Place

Saskatoon, Saskatchewan S7N 5C9 Canada

ABSTRACT

The Communications Security Establishment (CSE) is Canada's foreign signals intelligence (SIGINT) agency. Its empowering act prohibits the intelligence agency from collecting signals intelligence (SIGINT) on Canadians and collecting Canadian information. However, CSE is authorized to collect Canadian information under several mandates. This thesis examines CSE's adherence to its legal restrictions by analyzing its policies, oversight reports, and past actions. CSE is a relatively unknown and opaque agency, making past research scarce and researching the agency inherently difficult. This thesis attempts to shed light on the agency by analyzing how it collects, stores, uses, and disseminates Canadian information at the policy and practice level. Despite legal safeguards, evidence suggests that CSE routinely collects and shares Canadian information, raising questions on the validity of its prohibition. This thesis analyses the complexities of balancing national security and privacy concerns regarding CSE's mandate and activities to determine if CSE protects Canadians' privacy while fulfilling its national security raison d'etre.

ACKNOWLEDGEMENTS

This thesis would not have been possible without the guidance and support from my supervisor, Dr. Bell. Dr. Bell is a mentor without equal and I consider myself very lucky to work with her. Dr. Bell has been my biggest supporter during every step of this thesis, and I am truly grateful for her belief in myself and this thesis.

I would also like to thank the Department of Political Studies for their support throughout my time in the master's program. I would like to thank Alex, Cynthia, and Daniel for their support and advice which got me through many late nights writing.

Lastly, I thank my parents, whose unwavering support allowed me to reach this point.

Table of Contents

LIST OF FIGURES

LIST OF ABBREVIATIONS

ATIP – Access to Information and Privacy

CAFINTCOM – Canadian Forces Intelligence Command

CBSA – Canada Border Services Agency

CII – Canadian Identifying Information

COMINT – Communications Intelligence

CSE – Communications Security Establishment

CSEC – Communications Security Establishment Canada

CSIS – Canadian Security Intelligence Service

DND – Department of National Defense

ELINT – Electronic Intelligence

FINTRAC – Financial Transactions and Reports Analysis Centre of Canada

FISA – Foreign Intelligence Surveillance Act

FVEY – Five Eyes/Five Eyes Intelligence Sharing Alliance

HUMINT – Human Intelligence

IC – Intelligence Commissioner

NATO – North Atlantic Treaty Organization

NSA – National Security Agency

NSIA – National Security and Intelligence Adviser

NSICOP – National Security and Intelligence Committee of Parliamentarians

NSIRA – National Security and Intelligence Review Agency

OCSEC – Office of the Communications Security Establishment Commissioner

RCMP – Royal Canadian Mounted Policy

RFA – Request for Assistance

RFI – Request for Information

SCI – Sensitive Compartmented Information

SCIDA – Security of Canada Information Disclosure Act

SI – Special Intelligence

SIGINT – Signals Intelligence

SSO – Singal Source Operation

TELINT – Telemetry intelligence

1. Introduction, Theoretical Framework and Research Methodology

1.1 Introduction

The Communications Security Establishment (CSE) is Canada's Signals intelligence agency. Its primary role is foreign intelligence. In its role as a foreign intelligence agency, it has legal restrictions on targeting Canadians and the collection of Canadian information. However, CSE has several legal and policy allowances that allow it to collect Canadian information. This leads to the guiding research question explored in this thesis: does CSE collect Canadian information and respect Canadians' privacy?

In this thesis, I assess whether the CSE follows its own policies and procedures. I then conclude with some broad discussion of how these policies align with the theory of just surveillance or not. I use two theoretical lenses to explain *how* CSE collects information and *if* the possible violation of privacy resulting from the collection is justified using Petit's concept of *techno-securitization* and MacNish's principles of just surveillance respectively. Several findings are revealed through the study of CSE documents. First, several rules constrain CSE's collection, use, and distribution of Canadian information, there are many exemptions to these rules. For example, when CSE supports a government agency, they are beholden to the powers and restrictions of the agency they are supporting. In other words, while CSE may be restricted from directly targeting Canadian's, supporting the RCMP to target a Canadian's communications overrides CSE's restrictions. Secondly, the policies and procedures of CSE provide a high degree of discretion for analysts regarding the retention of Canadian information and what would be classified as "Canadian," making determining what Canadian information is retained by CSE possibly influenced by bias or prejudice. Lastly, oversight and review agencies reports show that, in previous reviews, CSE failed to share information required to determine if CSE was following its privacy restrictions, making verification of CSE's actions difficult (Office of the Communications Security Establishment Commissioner 2008, 9). Overall, the findings of this thesis show that CSE has measures to protect the Canadian information it retains; however, CSE at times failed to follow its own policies and showed gaps in its protection of Canadian information.

CSE is a rarely studied intelligence agency when compared to its American counterpart, the National Security Agency. The world of intelligence is inherently opaque to the average person. However, intelligence agenies, especially Signals Intelligence agencies like CSE, have the capability to collect vast amounts of information. To the average person, the potential impact of such practices may be the subject of speculation but understanding is often thin. Moreover, the agencies rarely disclose what information is collected or how they protect the rights of the public, in this case Canadians. As such, how this information is used, protected, and who sees it is only known to the agencies themselves.

The majority of the scholarship around CSE focuses on leaked information or publicly available information. Currently, there is a lack of scholarship on the policies of CSE and its impact on Canadians' privacy. As policies are vital instruments to the day-to-day actions of CSE, they need to be studied to gain a fulsome understanding of CSE's collection, use, and handling of Canadian information. This thesis aims to address a gap in scholarship on CSE by analyzing its policies and policy practices so as to provide transparency on how CSE impacts Canadian privacy.

1.2 Theoretical Framework

To explore the question of whether CSE collects Canadian information and respects Canadians' privacy, I draw on the concept of securitization. Securitization seeks to explain the process through which security actors give sufficient salience to a perceived threat that the public deems the threat dangerous enough for the security actors to address it (Balzacq, Léonard and Ruzicka 2016, 494). The security actors thus convince the public that an entity, be it a group, organization, or another state, is a dangerous enough threat that they need to combat it in the way they see fit, including through exceptional measures. Securitization theory argues that security actors form a narrative around groups and entities to make the audience view the target group as the security actor does (Balzacq, Léonard and Ruzicka 2016, 497). This thesis frames CSE's mandate and raison d'etre through a lens of securitization. With securitization theory, I will analyze the development of CSE's technical abilities and its employment of surveillance/ intelligence powers.

In the digital age, CSE can view and follow almost every aspect of a person's life if it chooses to devote the appropriate resources. CSE and other Five Eyes members' technical abilities do not focus solely on individual targets; the Snowden leaks show that the big data or mass collection of

data is possible and is carried out by Five Eyes intelligence agencies (Clement, Limits to Secrecy 2021, 132). The state of collection capacity is so robust that agencies need specialized tools, such as XKEYSCORE, to find relevant data. Using *techno-securitization* as the theoretical context, I will explore the pathways used by CSE and other SIGINT intelligence agencies to amass the technical ability and permission to access every aspect of a person's life.

According to Petit, *techno-securitization* refers to the securitization of technology to securitize everyday life. Scholars have examined how states produce securitization discourses around terror attacks to push for further security and surveillance measures. Petit argues that the securitization of technology has resulted in *everywhere surveillance* (2019, 32). As they show, the shift to protect against perceived threats and dangers has led states to securitize technology pre-emptively. Furthermore, *techno-securitization* feeds on itself to a point where the human element of enacting securitization is removed. Petit uses an example from Weber in which datasets and algorithms identifying possible threats during the war on terror show how threats are now countered by technical exploitation and formalized processes of trial and error, creating a discursive production of targets or threats (Weber, 2015, as cited by Petit, 2019, p. 34). Furthermore, this discursive production of threats allows security actors to justify their actions as acts of protection against these threats.

Petit argues that *everywhere surveillance* has three aspects. The first is that *everywhere surveillance* occurs on a global scale, as shown by the Snowden leaks (Petit 2019, 49). The Snowden leaks reveled the global nature of state-level surveillance, such as FAIRVIEW[1] (Greenwald 2014, 104). The leaks showed the extent of NSA's Global Access Operations wherein "….in just thirty days the unit had collected data on more than 97 billion emails and 124 billion phone calls from around the world" (Greenwald 2014, 92). Second, *everywhere surveillance* is a potentiality. That is, almost every piece of technology has the potential to be used as a tool for surveillance (Petit 2019, 49). At a personal level, security agencies can use a cell phone as a "roving bug" by remotely activating the microphone and listening (Greenwald 2014, 37). A person's social media can also be used to create "patterns of life," photos and videos from private accounts, and personal connections (Greenwald 2014, 161). Third, *everywhere*

[1] FAIRVIEW was one of the many global surveillance programs leaked in 2014. In 2014, FAIRVIEW collected massive amounts of metadata, via international communications cables, internet routers and switches, from a single "corporate partner" (Greenwald 2014, 104).

surveillance includes the complex geographies of surveillance. Almost anything, anywhere, can become a surveillance site, from internet backbones to a personal phone, thus subsuming it into the global surveillance infrastructure (Petit 2019, 50). Thus, techno-securitization shows how technology has become an integral part of securitization. From this lens, it is possible to demonstrate why and how CSE has been able to gain unprecedented power over information and why the Canadian state sees it as vital to its security.

1.3 Research Method

CSE is a government institution and intelligence agency, but its inner workings are not public-facing. Documents from CSE are one of the few ways researchers can access the agency's inner workings. As such, I use content analysis because it facilitates the systematic analysis of textual information (Halperin and Heath 2020, 372). Content analysis is an unobtrusive research method that allows research to be conducted without needing interviews (Halperin and Heath 2020, 374). Furthermore, I chose content analysis because government documents are my primary object of analysis. It allows for the systematic analysis of high-level trends and changes in organizational policy and procedures over time. By conducting a content analysis, I was able to thematically categorize key CSE documents used in this study. I first scanned the documents to determine the function of the documents and sources. I then categorized the documents based on common categories. I found the following categories or themes: policy, legal, and reviews. Some documents, such as slide shows, did not fit into these categories; however, some uncategorized documents were used as supporting evidence in the main three categories.

The large scale of documents reviewed in this thesis prohibits case studies. The BCCLA request, in which I found most of my research, had totaled over 4900 pages over 284 different documents. My own requests had dozens of documents. The documents used also do not contain all information, as almost all documents have redactions. Furthermore, the relevance of the documents limits the available information that could be used for research. Not all documents available focus on the use of Canadian information. This leads to excessive research time to filter relevant documents.

1.3.1 Freedom of Information

I gathered the majority of documents through the federal government's Access to Information and Personal Information (ATIP) regime. All primary sources used in this thesis are government

documents requested though ATIP requests and subsequently (and often after considerable delay) released. The ATIP regime is a freedom of information regime for citizens to request the disclosure of government information such as documents and data. ATIP provides access to some of the inner workings of government, which would not be accessible otherwise, as the Canadian government does not proactively release documents such as memos, nor does it have an automatic declassification regime for classified documents like in the USA. The lack of proactive transparency means that researchers studying Canadian government institutions are limited to requesting documents from the agency they are researching. As well, information can be exempted by government agencies. The *Access to Information Act* allows multiple exemptions to prevent information from being released under ATIP requests. Information that is perceived by CSE to be injurious to international affairs and the defence of Canada is exempted under section 15 (1). In the documents accessed in research for this thesis, most redacted information was withheld under this exemption.

Additional documents were gathered from several original ATIP requests and documents from requests made by others. Original ATIP requests, especially regarding classified information, take a long time to receive. For example, when requesting the updated version of the OPS-1 policy suite used for research in this thesis, CSE requested an extension of 152 days to complete the request. This delay limited the amount of documents that could be used for analysis. Some requests can take months to be received after the initial request. Due to the extended timeline for original ATIP requests, large portions of the documents used by this thesis are from previous ATIP requests. A large portion of the documents used were from a major ATIP request by the BC Civil Liberties Association. I also used the FOI request database from the Secret Canada project to find past requests from CSE.

1.3.2 Redacted Information

The nature of the research material used in this thesis presents several inherent limitations in gathering information. National security documents and documents produced by intelligence agencies are highly classified. Most documents in this thesis's research are classified as "SECRET" or higher. Furthermore, some documents are classified under Special Compartmentalized Information (SCI) regimes, such as Special Intelligence (SI), sometimes referred to as "above top secret." Said documents contain SIGINT information and are heavily

redacted. Redactions of information present a significant barrier to many researchers. ATIP documents are released once all classified information is removed, limiting the knowledge that researchers can gain about the subject matter under investigation. As there is no automatic declassification regime in Canada, all documents, no matter how old, are reviewed by the government and have classified information removed. The lack of proactive or historic declassification further limits the analysis of government documents as all documents, no matter how old, must go through the same time-intensive declassification review process before being released under a request.

However, researchers can garner some information from the lack of it. Nath argues that a lack of information is information in itself (Nath 2014, 22). Furthermore, Nath argues that by comparing redacted information to non-redacted information, a comparison of the two types of information can be revealing (Nath 2014, 23). For example, if one torture method is non-redacted, but other methods of torture appear to be redacted, one can compare what information the state declares to be secret and speculate on both the information that is redacted as well as the state-level reasoning to determine was to be kept secret. In as example provided by Nath, in one memo, the use of releasing bugs in a cell is not redacted, while other methods of torture within the memo are (Nath 2014, 25). The comparison of redacted and non-redacted information leads Nath to reasonably conclude that the redacted torture methods are much worse than the non-redacted torture methods. Predictably, the state removes information from the public version of the document that the state does not want the public to know and due to the concerns, that knowing might evoke among citizens, groups, or other states. While redacted information is normally a barrier for researchers, it also provides insight into the "mind" of the state. Redacted information is an object that represents information the state wants to keep hidden.

This thesis proceeds as follows. Chapter 2 will provide context about CSE and its role by discussing what SIGINT is, CSE's history, and CSE's operational landscape. Chapter 3 will outline previous literature on CSE, legal aspects of intelligence and CSE, and the question of ethical surveillance. Chapter 4 explores the concept of privacy and will define it within the context of digital information. Chapter 5 will analyze the findings of my research using primary documents, covering policy and reports from CSE and its review and oversight agencies. Lastly, in chapter 6, I will analyze the findings from chapter 5 using the theories of *techno-securitization*

and Macnish's framework of just surveillance from chapter 4. From this analysis, I determine that while CSE collects Canadian information, it respects Canadian privacy as long as it follows both wider government regulations and its own policies. CSE fails in its requirement to protect Canadians' privacy when it fails to follow its own policies and controls.

2. SIGINT, CSE, and the Canadian Intelligence Community

As Canada's SIGINT agency, CSE is part of the broader Canadian Intelligence Community. The Canadian Intelligence Community comprises several intelligence-producing agencies, and many more agencies and departments use CSE's SIGINT. Furthermore, CSE maintains many international partnerships with other SIGINT agencies. However, the Canadian Intelligence Community and SIGINT are highly technical areas. This chapter aims to develop an understanding of the nature of CSE's work, its operational contexts, and its relationships with domestic and international partners. This chapter will explain signals intelligence, the background of CSE as an organization, the Canadian intelligence community, and CSE's international partnerships, such as the Five Eyes.

2.1 SIGINT

SIGINT, or Signals Intelligence, is quickly becoming the premier form of intelligence in our increasingly digital world (Gill and Phythian 2018, 80). In the digital world, it is more effective for states to use electronic intelligence and surveillance over human intelligence. States can use the same tools for one target and easily shift their capabilities to another target without heavy use of resources. In contrast, human intelligence (HUMINT), in which shifting of intelligence priorities requires finding a new asset in the target area or organization, requires significantly more resources (Gill and Phythian 2018, 80). It is not that HUMINT does not have an important role in the current intelligence world but rather that SIGINT provides vast amounts of information in contrast to other intelligence-gathering methods.

SIGINT contains three subfields: Communications Intelligence (COMINT), Telemetry Intelligence (TELINT) and Electronic Intelligence (ELINT) (Gill and Phythian 2018, 68). This thesis focuses on CSE's use of COMINT. COMINT comes from the interception of telephone, internet or radio communications (Gill and Phythian 2018, 68). SIGINT is the targeted or bulk collection of communications or metadata, the targeted or bulk collection of content, and the targeted or bulk exploitation of computer networks (Gill and Phythian 2018, 69-70).[1] In other words, SIGINT via COMINT focuses on collecting content and metadata.

[1] Also known as hacking.

Metadata is information on data. For example, metadata of a call between two people would be the length of the call, the sender, the receiver, and information on the phones used. Metadata does not record the content of the communication; it only records the nature of the communication. Content collection is the collection of the content of the communication. Content collection consists of "wiretapping" calls, text content, social media messages, emails, etc. Both methods of surveillance provide intelligence. Metadata can give insight into a target's social network without using the resources required to collect the content of every communication they send. In contrast, content collection, although more resource-intensive, allows for collecting a deeper level of information once a person is targeted.

SIGINT goes beyond directly targeting individuals. With the world becoming more connected to the internet in the digital age, SIGINT has also begun to evolve to adapt to technological changes such as bulk data collection, also known as "big data" or "mass surveillance." The Snowden leaks exposed the vast array of NSA bulk data collection, which included data collected by members of the Five Eyes alliance. Bulk data collection has become a valuable part of the SIGINT production chain. The ability to collect and store mass amounts of metadata provides intelligence analysts with extreme insight into what is happening worldwide.

Furthermore, bulk data collection acts as a discovery tool that intelligence agencies use to identify new targets (Gill and Phythian 2018, 16). The Snowden leaks included a slide revealing that the NSA bulk data collection captured 60% of content and 75% of metadata (Ogasawara, Collaborative Surveillance with Big Data Corporations 2021, 28). This is a vast volume of traffic and information at the state's disposal, and it can be assumed that the bulk collection capabilities of the Five Eyes partners have increased since the Snowden leaks of 2014. Other leaks have exposed how the NSA, and presumably the rest of the Five Eyes, can capture such large amounts of information. For example, the NSA has several agreements with telecom providers to allow it to connect to the internet and telecom hubs. These hubs funnel a massive quantity of communications and data. The NSA has covert connections to these hubs that send copies of the data straight to NSA servers (Ogasawara, Collaborative Surveillance with Big Data Corporations 2021, 24-25).

Clement (2021) notes that in 2012, it was exposed that CSE tracked devices using Wi-Fi hotspots in Canadian airports. To do so, CSE did not attach sensors to airport networks; instead, CSE

collected internet traffic metadata. CSE then searched metadata for the traffic from airport networks (Clement, Limits to Secrecy 2021, 130).[2] In addition, the Snowden leaks revealed CSE's program CASCADE.[3] The EONBLUE and INDUCTION sub-programs of CASCADE captured around 10 gigabytes per second of data per network line using deep packet inspection[4] (Clement, Limits to Secrecy 2021, 132). EONBLUE captured both metadata and content of collected data (Clement, Limits to Secrecy 2021, 132). The reveal of CASADE showed that CSE, like the NSA, used its access to telecom companies to install sensors to capture vast amounts of data from network backbones. These sensors were located within Canada, capturing Canadian network traffic (Clement, Limits to Secrecy 2021, 132). Clement notes that the CASADE documents were from 2012; but again, it is reasonable to assume that CSE has only increased its data collection capabilities (Limits to Secrecy 2021).

2.2 CSE

As noted in the introduction, the Communications Security Establishment (CSE) is Canada's SIGINT and cybersecurity agency. CSE evolved from the Communications Branch of the National Research Council. The Communications Branch was tasked with intercepting radio communications, breaking encryption and ensuring the Canadian government's communications were encrypted. The Communications Branch first found its role during World War Two. However, during the Cold War, the need for SIGINT grew and, in tandem, so did CSE's precursor (Lyon and Wood, Introduction 2021, 10). In 1975, Canada's SIGINT agency was transferred to National Defense and became the Communications Security Establishment of Canada (CSEC). While CSE grew over the years, it was during the Harper government and post 9/11 that CSE evolved into a modern SIGINT agency (Robinson 2020, 73). During the Harper government, CSE moved from its smaller and older headquarters into its current multi-million-dollar headquarters, arguably a physical representation of CSE's increasing importance (Lyon and Wood, Introduction 2021, 10). The Harper government also passed several bills that increased the surveillance powers of CSE, RCMP, and CSIS. One example is the *Technical*

[2] CSE parsed out user ID's from the bulk internet traffic by using known airport network connections from network backbone sensors. CSE also used this method to conduct a proof of concept by using the same "needle in a haystack" analysis on a Canadian city's internet traffic (Clement, Limits to Secrecy 2021, 131).

[3] CASCADE is made up of four separate collection sub-programs: INDUCTION, EONBLUE, THIRD-EYE, and CRUCIBLE (Clement, Limits to Secrecy 2021, 132).

[4] Deep packet inspection is a method of inspecting the content of a data packet as it passes a network checkpoint. In other words, it is the ability to inspect the content of network traffic.

Assistance for Law Enforcement in the 21st Century Act, which gives law enforcement in Canada warrantless access to Internet communications (Lyon and Wood, Introduction 2021, 10). As part of CSE's mandate is technical assistance to law enforcement, warrantless access would be transferred to CSE when assisting law enforcement.

The initial form of CSE's current mandates was first put in place in 2001, which set out the original three-section mandate for CSE in the *National Defense Act*: Part A, Part B, and Part C. Part A is CSE's mandate to collect foreign intelligence. Part B is CSE's cyber security and information protection mandate. Part C is CSE's mandate to provide operational and technical assistance. Part A and Part C of CSE's mandates are the main focus of the research of this thesis because they encompass activities that are most likely to handle Canadian information. Part A sets out the restriction of CSE collecting Canadian information. Part C is where CSE's cooperation with domestic security agencies is formalized within its responsibilities. Before 2001, it was illegal for CSE to collect any communications that originated or terminated in Canada, and it "…could only target communications that originated and terminated in foreign jurisdictions, and which involved foreign intelligence" (*X(re),* 2013 FC 1275 at 14). In other words, CSE was strictly prohibited from collecting any Canadian communication before 2001. CSE gained the authority to collect communications that started or ended in Canada under its three mandates with the passing of the *Anti-terrorism Act* in 2001.

CSE's mandate was expanded with the passing of the *Communications Security Establishment Act* (CSE Act) in 2019 as part of the national security bill C-59. The new CSE Act introduced an additional mandate: Part D: cyber operations. This additional mandate allows CSE to conduct cyber attacks both proactively and defensively. Defensive cyber operations purportedly allow for CSE "activities" to protect Canadian and federal government infrastructure and systems.[5] Active cyber operations allow CSE to actively "… degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group…" (*Communications Security Establishment Act*, 2019). Furthermore, Section 32 of the

[5] The CSE act does not specify what constitutes activities but declares that they are defined in the Ministerial Authorizations allowing them. Furthermore, these authorizations are highly classified, meaning the activities are often redacted when published publicly.

act prohibits CSE from causing death or bodily harm or obstructing democracy or the course of justice (*Communications Security Establishment Act*, 2019).

Under section 22 of the *CSE Act*, CSE is prohibited from collecting Canadian information or information on persons in Canada as part of its foreign intelligence, cybersecurity, and cyber operations mandate (*Communications Security Establishment Act*, 2019). However, there is no prohibition on collecting Canadian information for its technical assistance mandate. As the assistance mandate is for law enforcement and security agencies, a prohibition on collecting Canadian information would severely limit CSE's assistance. Of particular note, this mandate allows CSE to assume the legal powers of the department or agency it assists (Communications Security Establishment 2019). For example, where CSE formally assists the RCMP, it subsumes the RCMP's surveillance powers. Likewise, the limitations placed on CSE include any restrictions placed on the RCMP, such as on a surveillance warrant. The legal powers of the requesting agency supersede any of CSE's restrictions and prohibitions legally. However, the question remains: how much Canadian information is collected by CSE under this mandate?

An adjacent consideration is the exceptions to the prohibition under the other mandates. Ministerial Authorizations allow CSE to carry out certain aspects of its mandate and to contravene acts of parliament. CSE may take actions that would be illegal under Canadian law, but such actions require CSE to have ministerial authorizations. In other words, CSE can be authorized by the minister to act against the law in the performance of its duties. Ministerial authorization is the process where the minister weighs the national interest of the actions requested and the privacy rights of Canadians. Ministerial Authorizations are reviewed and ruled on by the Intelligence Commissioner (IC) before CSE can act on the authorization. The IC reviews Ministerial authorizations to ensure the Minister made a reasonable decision in signing the authorization (Office of the Intelligence Commissioner 2023, 3). The Intelligence Commissioner may deny, approve, or require changes to sections of Ministerial Authorizations. For example, in a review of a Ministerial Authorization dated April 21, 2023, the IC approved the majority of the authorization while denying two sections of the authorization, as some of the activities were deemed out of scope under CSE's foreign intelligence mandate (Office of the Intelligence Commissioner 2023, 16). Having the IC as an oversight agency is a way for CSE to

ensure that it follows its own mandate and that CSE is not authorized to act outside of the scope of its mandate.

CSE's surveillance and intelligence powers are situated within several different acts of parliament, not just within its empowering act. The *CSIS Act*, *National Defense Act*, *Privacy Act*, and *Telecommunication Act*, among others, all have sections that give CSE legal powers of surveillance outside of its empowering act (Prince 2021, 45). Importantly, the many statutes empowering CSE and other security agencies in Canada result in an opaque legal landscape regarding surveillance. This limits both the accountability and transparency of security agencies in Canada to the public, as deciphering the legal bases for surveillance can be frustrating and difficult to clarify for both the public and, at times, the courts, as demonstrated further in this chapter. In addition to a complex legal landscape, the Canadian Intelligence landscape is also complex.

2.3 Canadian Intelligence Landscape

The Canadian Intelligence community host a wide array of departments. Among them, only CSE, Canadian Security Intelligence Service (CSIS), Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and Canadian Armed Forces Intelligence Command (CAFINTCOM) are the dedicated intelligence agencies of Canada. Each agency has its intelligence focus. CSE's focus is foreign signals intelligence, CSIS's mandate is security/human intelligence, FINTRAC is financial intelligence, and CAFINTCOM is DND's military intelligence unit. In addition to these dedicated agencies, core agencies guide the intelligence community as a whole. The Privy Council Office contains the National Security and Intelligence Adviser (NSIA), the Security and Intelligence Secretariat and the International Assessment Staff. The NSIA acts, as stated in the name of the role, as the primary adviser for the Prime Minister on national security and intelligence matters. The NSIA and their Staff, along with the Security and Intelligence Secretariat, act akin to the office of the Director of National Intelligence in the United States. They develop the national intelligence priorities of the federal government. Other departments play a core role in the Canadian Intelligence Community but are not intelligence production agencies. These departments, such as the Canadian Border Services Agency, use intelligence to perform mandated activities.

The Canadian Intelligence Community contains several oversight and review agencies that act as a check on the power of intelligence agencies. The Intelligence Commissioner (IC) oversees both CSE and CSIS (Office of the Intelligence Commissioner 2022, 9). They review Ministerial Authorizations and CSIS warrants to ensure they align with Canadian law and regulations. The ICO can deny or amend authorizations by the Minster of National Defenses or classes of datasets used by CSIS after a quasi-judicial review (Office of the Intelligence Commissioner 2022, 9).

The National Security and Intelligence Review Agency (NSIRA) reviews both CSE and CSIS. They review the actions of all government departments dealing with national security and intelligence. They also review any complaints submitted by the public regarding national security agencies, such as complaints about the activities of CSE and CSIS. The investigation into any complaints, including the content of complaints, is not public. Most recently, NSIRA reviewed CSE's Ministerial Authorizations and Ministerial Orders in 2023. NSIRA also reviews issues across the Canadian National Security and Intelligence landscape.

The National Security and Intelligence Committee of Parliamentarians (NSICOP) is the legislative review committee of Parliament. It conducts special reviews of the activities of national security and intelligence agencies. Furthermore, the committee conducts reviews at the request of government ministers. For example, in 2021, the Minister of Health referred the matter of possible security incidents at the National Microbiology Laboratory in Manitoba to NSICOP as it was a matter of national security (The National Security and Intelligence Committee of Parliamentarians 2022, 3).

Although the terrain of Canada's intelligence community is complex and multifaceted, the CSE has a core place within it. As Canada's sole SIGINT agency, CSE produces SIGINT reports for other government departments. As long as a department needs SIGINT reports, CSE provides access to them, including domestic security agencies like the RCMP and CSIS. Furthermore, CSE provides SIGINT reports to other government departments outside the Canadian intelligence community. For example, departments not generally associated with needing SIGINT have memorandums of understanding with CSE for receiving SIGINT. These departments include the Canada Revenue Agency and the Canadian Nuclear Safety Commission (Communications Security Establishment; Canada Revenue Agency 2008, Communications

Security Establishment; Canadian Nuclear Safety Commission 2009). CSE's partnerships go beyond domestic agencies and have many international intelligence partnerships.

2.4 International Partnerships

The primary role of CSE is to provide its domestic partners with SIGINT. CSE produces SIGINT through its means and with the assistance of its international partners. CSE's primary international intelligence partnership is the Five Eyes intelligence alliance, also known as FVEY. The Five Eyes alliance comprises the United States, the United Kingdom, Canada, New Zealand, and Australia. While other non-signals intelligence agencies are part of Five Eyes, the SIGINT agencies of these states are core members.[6]

The Five Eyes members have a formalized intelligence-sharing relationship with each other. This relationship started in World War II with the UKUSA agreement. As the Cold War progressed, more members were inducted into it (Lyon and Wood, Introduction 2021, 8), including Canada in 1948. The UKUSA agreement was a SIGINT-focused agreement, making SIGINT the core focus of the intelligence shared (National Security Agency n.d.). Five Eye members define themselves as "second parties" to show their cooperation. In contrast, intelligence agencies outside the Five Eyes are "third parties" (British Columbia Civil Liberties Association 2023).

As the most well-known intelligence alliance in the world, Five Eyes has vast technical and intelligence-gathering capabilities. Furthermore, a large volume of intelligence gathered by each member is shared or accessible to other members (Clement, Harkness and Raine 2021, 258). Notably, it has been argued that Five Eyes members conduct "jurisdiction shopping" to subvert their own domestic surveillance restrictions (Petit 2019, 40). While using the alliance to get the most surveillance access, the Five Eyes members also formally agreed not to spy on each other (Warner 2013) unless specifically subcontracted. For example, CSE asked Five Eye partners to spy on Canadians during the War on Terror. Leman-Langlois cites a specific case, *X(re)* (2013 FC 1275) (Leman-Langlois 2021, 62). In 2009, CSIS asked CSE to request its Five Eyes partners surveil a Canadian target abroad (*X(re),* 2013 FC 1275 at 42). The federal court found that

[6] These agencies are the National Security Agency (NSA) of the US, the Government Communications Headquarters (GCHQ) of the UK, the Australian Signals Directorate (ASD), the Government Communications Security Bureau (GCSB) of New Zealand, and the Communications Security Establishment.

CSIS's warrant did not allow foreign agencies to surveil a Canadian on behalf of CSIS (*X(re),* 2013 FC 1275 at 125).

In summary, CSIS was using domestic surveillance warrants to request that Five Eyes agencies surveil Canadian terrorist suspects abroad via CSE.[7] While the current legal framework allows this, the surveillance sub-contracting by Five Eyes was initially left out of the interception warrants (Leman-Langlois 2021, 62). This case highlights the legal complexities of CSE's international intelligence sharing when it involves Canadians. Also evident is that the Five Eyes partnership is an integral source of intelligence for CSE. However, since little is known about the extent to which it plays in the day-to-day relationship to domestic surveillance of Canadians, its impact on privacy is relatively unknown.

2.5 Conclusion

The world of SIGINT and Intelligence is complex and technical. Intelligence and security agencies with varying privacy impacts can access many different types of information. As an organization, CSE has a complex history outside of the public eye. After 2001, in an increasingly digital world, CSE became more prevalent in the Canadian intelligence community through its international partnerships with the Five Eyes.

CSE is still a relatively unknown agency to Canadians, only recently making itself more present in the public eye. The Government of Canada did not acknowledge CSE's existence until 1983, and CSE's most public-facing unit, the Canadian Center for Cybersecurity, was established in 2018 (Communications Security Establishment n.d.). This makes the study of the CSE a relatively niche topic in academia. While there is a body of research on Canada's national security community, there is limited focus solely on CSE. In the next chapter, this thesis will review scholarly studies on CSE, focusing on CSE's legal and policy landscape, how its conduct and capabilities have been made sense of, and the connections that scholars have posed between privacy, intelligence and state power.

[7] The court found that CSIS getting a" Section 12" warrant, then asking for Five Eye support via CSE's Assistance mandate was not legal under the current CSIS warrant regime.

3. LITERATURE REVIEW

While CSE is a relatively unknown intelligence agency, a relatively large amount of literature surrounds it. I have separated the literature on CSE into three themes: Legal and policy, CSE actions and capabilities, and the relationship between privacy, intelligence, and the state. These themes relate to the historical, legal, and policy contexts around CSE. This chapter will also explore the relationships between the three themes to develop an understanding of how each plays a role in CSEs and why it impacts Canadians' privacy. The legal context of CSE develops an understanding of the state of research on the legality of CSE's activities. At the same time, the policy shows what other research has found on the day-to-day aspects of CSE actions. The themes of privacy, intelligence, and the role of the state were chosen to understand how each of these ideas inform and impact each other. I will work to develop the idea of what privacy means by understanding how the state seeks to protect itself from perceived threats while conflicting with its commitment to protect privacy.

3.1 Legal Issues and Policy

The first theme of the literature is the legal and policy analysis of CSE's intelligence. CSE receives its mandate from the *Communication Security Establishment* Act (2019). CSE is prohibited by law from collecting Canadian information, officially called Canadian Identifying Information (CII), under the act (West 2020, 82-83). However, the act allows for exceptions to this prohibition.

The first subsection of the act concerns the legal mandate of CSE and other Canadian intelligence agencies and how it has evolved over time. The current literature focuses on Bill C-59, a relatively new piece of legislation which overhauled the mandate of CSE and provided it with additional powers (Williams 2020, 133). These changes are analyzed by Williams, who emphasizes the importance of striking a balance between what CSE can collect legally in the name of national security versus the right to privacy (2020, 249). The balance Willams refers to is the need for national security and the rights of Canadians guaranteed under the Charter,

specifically privacy.[1] The government argued that Bill C-59 allows CSE to protect Canada against current threats. However, Willams states that this rationale does not make up for deficient privacy safeguards. Also, the secret history of CSE, its existence being hidden from Canadians for most of its time as an agency; leaves a lack of public record and information gathering programs under the Fives Eyes, giving Canadians little reason to trust CSE (2020, 151). Willams argues that while some privacy safeguards can make allowances for national security, the powers CSE was given are too broad. Further, they note that these deficiencies are combined with a lack of additional privacy safeguards. One example of additional privacy safeguards left out of the act is the lack of inclusion of the Privacy Commissioner in any oversight or watchdog role, leaving only the intelligence and national security watchdog agencies in this role. Arguably, leaving the privacy experts within the federal government, who expressed they should have an oversight role, out of CSE's oversight regime infers a limited commitment to the protection of Canadians' privacy. These two issues – the extended powers of CSE and inadequate privacy safeguards to avoid rights violations – strike an unreasonable privileging of national security over privacy.

As noted earlier, CSE has four mandate sections. Under section C, the technical and operational assistance mandate, CSE assists domestic law enforcement agencies. Robinson notes that between 2009 and 2012, CSE received 294 requests under this mandate. Approximately 70% of these requests were from CSIS (2020, 77). The rest of the requests came from the RCMP, the CBSA, and DND. Furthermore, all requests regarding monitoring communications for external departments came from CSIS (Robinson 2020, 77). As CSIS is a domestic security agency, it is assumed that the majority of requests involve individuals located in Canada. This is a direct contradiction of CSE's prohibition of targeting Canadians. However, under its assistance mandate, CSE subsumes the powers of the agency it is assisting, making its actions taken on behalf of CSIS legal if they are legal for CSIS. This issue raises serious questions about the legal and policy implications of a mandate that authorizes CSE to act in seemingly contradictory directions.

The legal landscape for intelligence agencies in Canada has changed dramatically since 2001. Ogasawara (2022) argues that Canada has endured three phases of legal changes to allow for

[1] Section 8 of the charter guarantees: *Everyone has the right to be secure against unreasonable search or seizure*. It is understood that search means both tangle and intangible things, such as electronic information (Department of Justice n.d.).

legal surveillance. The first phase is the post-9/11 era when the European Convention on Cybercrime was signed. Although Canada is a non-member of the convention, during this phase, Canada, along with other signatories, used the convention to grant law enforcement legal access to data traffic. In other words, the convention was used as reasoning to weaken legal data privacy protection (Ogasawara, Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence 2022, 327). However, Ogasawara notes that several bills attempting this did not pass in parliament, such as the *Modernization of Investigative Techniques Act* in 2005. Yet, it was revealed that CSE conducted mass collection of metadata secretly through ministerial orders from 2005 onwards (Ogasawara, Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence 2022, 327). The inability to pass surveillance legalization links to the next phase of legal reforms in Canada.

According to Ogasawara, the second phase is resistance from the courts and increasing questions of accountability. The Harper government passed the *Protecting Canadians from Online Crime Act* in 2013. The act allowed telecommunication companies to voluntarily share metadata with the government when they suspected illegal activity by a customer. The subsequent Supreme Court ruling, *R v Spence,* changed the act. This ruling set a precedent for law enforcement to need a warrant when receiving information from telecom companies, even when the sharing is voluntary. Furthermore, the courts found that CSIS asked CSE to request its foreign partners to spy on Canadians aboard. Through "jurisdictional shopping" – a concept denoting the practice of working with allies to circumvent domestic restrictions – CSIS conducted surveillance without domestic restrictions (Whitaker 2015, 215). Ogasawara quotes Whitaker, who terms the use of foreign partners to get around domestic restrictions as "guerrilla accountability" (Whitaker 2015, 215). The use of guerilla accountability, Whitaker argues, allowed the Five Eye partners to attest that they do not surveil their own citizens, only foreigners. When a federal judge discovered this questionable claim by Five Eyes and determined it illegal, the federal government appealed. However, during this time, the Harper government changed CSIS's empowering act, making the practice legal (Whitaker 2015, 216). Ogasawara argues that the Harper government passed this law in response to the parliament hill shooing in 2014, using a time of crisis to expand CSIS's surveillance powers outside of Canada (Ogasawara, Legalizing Illegal Mass Surveillance: A

Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence 2022, 330).

The third phase, according to Ogasawara, started with the passing of the *Anti-Terrorism Act* in 2015.[2] Ogasawara notes that changes to the *Canadian Security Intelligence Service Act* by the *Anti-Terrorism Act* legalized previously illegal surveillance activities. The Anti-Terrorism Act allows CSIS to act against threats to Canada, regardless of the Charter of Rights and Freedoms (Ogasawara, Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence 2022, 330). Ogasawara uses the Canadian Civil Liberties Association analysis that C-51 allows CSIS to wiretap private conversations to investigate extremist speech, which violates the right to free speech (Canadian Civil Liberties Association 2015). Ogasawara argues that these changes removed the difference between domestic and foreign intelligence collection and any protections enjoyed by Canadians by being on Canadian soil were consequently removed (2022, 331). This phase also allowed CSIS to conduct illegal surveillance by integrating the judiciary. CSIS currently has judges sign off on pre-authorizations of illegal activities, granting them immunity when CSIS activities violate the law. This regime is akin to the CSE ministerial authorization framework. The CSE ministerial authorization regime has the Minister of National Defense sign an authorization allowing CSE to conduct usually illegal acts; the authorization is then quasi-judicially reviewed before being enacted.

In her chapter, *Lawful Illegality* (2015), Austin expands on the legal reasoning that underpins CSE's metadata surveillance program, as discussed above. Austin notes that CSE claimed that its metadata collection program was legal. However, the legal interpretation CSE used is classified and thus is not available for public review (Austin 2015, 107). Furthermore, CSE claimed that it was held to account by the Commissioner of CSE, its oversight at the time. However, Austin argues that when there were differences of opinion between the Commissioner and CSE on the legality of CSE's actions, CSE would prevail (Austin 2015, 107). Austin further argues that CSE's lawfulness is the claim that they operate within their interpretation of the law (Austin 2015, 108).[3] Since legal advice and decisions on intelligence are classified and not

[2] The *Anti-Terrorism Act* was passed twice, first in 2001 and in 2015.

[3] It should be noted that the legal and oversight framework was fundamentally changed with the passage of the *CSE act* in 2019.

public, it is a one-sided legal review as there is no one to contest the decision (Austin 2015, 108). The closed nature of legal decisions, along with the complexity of the different mandates of CSE, make determining if CSE is following its prohibitions by observers outside of CSE and the intelligence community difficult.

The second major piece of legislation reviewed is the *Security of Canada Information Disclosure Act* (SCIDA), which allows government departments to share information about national security threats. Through SCIDA, along with other legal regimes, notes West, CSE shares the information it gathers with domestic partners, such as CSIS and the RCMP (2020, 82). The fact that CSE shares information has several legal implications, as the *CSE Act* prohibits CSE from collecting Canadians' information.

The second subsection of the legal-focused literature is the review of the oversight and review framework for CSE. In 2019, Bill C-59 overhauled the oversight and review framework for CSE and Canadian intelligence agencies. The main changes were the creation of the Intelligence Commissioner (IC) and the National Security and Intelligence Review Agency (NSIRA) (West 2020, 258). These were formed from the previous agencies of the Commissioner of CSE and the Security and Intelligence Review Agency, respectively. West usefully details the mandate differences between review and oversight agencies and what accountability means. As she explains, a review agency reviews the actions of a government department after the fact, while an oversight agency determines if the actions are appropriate in real-time (West 2020, 258).

3.2 CSE Actions and Capabilities

The next theme of the literature about CSE is the intelligence-gathering capabilities of the agency. These sources mainly focus on the actions of CSE revealed in the Snowden leaks. These leaks provided information that would otherwise be classified to the general public. The highlight of these revelations was the project codenamed EONBLUE, which was the passive collection of information by CSE (Geist 2015, 80). CSE has the capability to collect vast amounts of internet metadata both in Canada and the world through the CRUCIBLE program

(Parsons and Molanr 2021, 241).[4] The study of such information provides access to information otherwise not available. The passive collection of SIGINT by CSE highlights the privacy risks that come with the all-encompassing nature of SIGINT collection. Passive collection is akin to hooking a wiretap to an internet line and collecting all the information going through it. This form of collection runs the obvious risk of collecting Canadian information. CSE does have several policies to deal with this issue, but critical analysis by researchers questions the effectiveness of mitigating efforts. The literature also discusses the privacy implications of mass government surveillance overall. Parsons (2021) provides a detailed analysis of the relationship between privacy and SIGINT. For example, Parsons explains the privacy distinctions between a person's private and public life and how SIGINT violates a person's privacy if only the collection of metadata is done versus the collection of communications (2015, 3-4). Parsons states that privacy is a boundary concept with three separate boundaries. First is spatial boundaries in physical areas such as a home. Second is behavioural boundaries in areas with unwanted attention, such as medical or sexual behaviours. The last is informational boundaries, covering a variety of personal information that requires protection, such as sexuality or religion (Parson 2015, 4). Furthermore, Parsons states that to determine if a privacy boundary is harmed by surveillance, evidence is needed to assess if privacy has been or potentiality violated. Linking his argument to SIGINT and metadata, Parsons states that the vast quantity of metadata collected by SIGINT agencies allows them to "out" or reveal substantive information on a person without the need for direct capture of communications (Parson 2015, 4). The privacy impact of capturing metadata raises the question of when metadata collection becomes a privacy violation. This is because SIGINT analysts can correlate metadata to determine if they have a need to request further and more intrusive collection methods. This is seen in some of the documents from CSE, where CSE SIGINT analysts use the least intrusive methods first and then use more intrusive methods of data collection to determine if a target is Canadian (Communications Security Establishment 2014, 2).

The literature on CSE's actions evinces mixed perspectives on whether CSE is invading the privacy of Canadians. On one side, there is the analysis that concludes that CSE does not have the resources to monitor Canadians superfluously, as determined by Rimsa (2011, 131) in

[4] The CRUCIBLE program was a metadata collection program on non-government networks (Parsons and Molanr 2021, 241).

Eavesdroppers. Rimsa's argument lends to the fact that CSE is a relatively small intelligence agency, even within the Canadian Intelligence community, and does not have the power or fiscal resources to monitor Canadians without a justification (Rimsa 2011, 132). However, at the same time, CSE has monitored Canadians "with justification." Rimsa uses the CSE monitoring of the Mohawk Warrior Society in 1993-94 for possible weapon shipments as an example (2011, 134). This point links to the side of the literature that argues that CSE monitored Canadians within Canada in the past.

The capability of CSE as a SIGINT intelligence agency is revealed in the Snowden leaks. As a FIVE EYES member, CSE information was included in the leaked documents, presenting an important opportunity for research on CSE's surveillance and collection practices. Scholars, such as Geist, found that CSE's information collection capabilities within Canada are highly developed and linked to the major telecom providers in Canada (Geist 2015, 81). For example, the leaks showed that CSE could intercept Canadian internet traffic within Canada and had access to major internet hubs run by the biggest telecom corporations in Canada, such as Bell and Rodgers, as shown by Lyon and Wood (2021, 140).

3.3 Privacy, Intelligence and the State

The relationship between privacy and intelligence is complex. Before analyzing the relationship between intelligence and the state, privacy *itself* needs to be understood. Miller and Walsh (2016) define privacy as a moral right of a person regarding "[i] the possession of information about themselves by other persons; or [ii] the observation/perceiving of themselves by other persons" (2016, 195). They further define privacy as part of the right of autonomy. Autonomy is the right to control who to exclude or include regarding one's personal information. Privacy is a human right in both the UN *Charter of Human Rights* and the Canadian *Charter of Rights and Freedoms* (Bannister 2005, 66). However, scholars have also noted that the right to privacy has shifted in the age of the Internet. Our personal data, our interactions with the internet, and our personal communications are all now stored and processed at a massive growing scale (Wisnewski 2016, 205). Literature on electronic surveillance and privacy shows that states need to balance the right to privacy and the security of the state when conducting electronic surveillance (Bannister 2005,

65). The powers of the state to collect information are vast, and as such, the amount of information the state can gather on persons is vast.

As the relationship between technology and privacy is complicated in our digital world, CSE would not have the ability to peer into our lives if not for our relationship with technology. Wisnewski notes that we live in an electric panoptic state in which how we are, what we do, and what we think is revealed through our data (2016, 205-206). Wisnewski argues, however, that even with all of our data being collected, almost no one is actively using it. The data is anonymized and often deleted after a period of time. Wisnewski links this reality to the prevalence of security cameras, which has reduced their panoptic impact. Their ability to change how people act is reduced as people assume no one is actively watching them. People only change how they behave when they believe they are *actively* watched.

Further, as Bannister (2005) delves into the complex relationship between technological surveillance and privacy, he argues that there is always a trade-off between privacy and the state needing to protect itself (Bannister 2005, 65). No community is completely private, and some elements of privacy inevitably must be sacrificed to be a member of a community, like a state. Bannister (2005) argues that:

> If A is not reporting all his taxable income or is making a bomb in the basement with a view to blowing up the local police station, he is hardly likely to advertise either fact. In order to detect this, society has to take some sort of pre-emptive action such as accessing his bank records or breaking into A's house. Given the legal principle that somebody must be assumed innocent until proven guilty, it is easy to see how the question of a 'right' to informational privacy quickly degenerates into a grey area where delineation of clear and unambiguous laws or principles is exceedingly difficult (66).

However, Bannister clearly states that the risk of unauthorized intrusion into privacy is real. He notes that the NSA's ECHELON program and jurisdictional agreements between states to bypass domestic surveillance restrictions are notable examples of the lengths that states will go to collect data on their citizens.[5]

[5] For context, Bannister wrote his article in 2005, before the Snowden leaks in 2013.

Bannister and Wisnewski approach the question of digital privacy with two different lenses. Bannister weighs risk and privacy, while Wisnewski considers consent and privacy. Wisnewski argues that the internet is not a private domain; it is public, and internet activity is not inherently private. Furthermore, Wisnewski argues that the idea of consent is different when it concerns private internet companies versus government; governments, they suggest, are inherently different. By using a service or agreeing to terms of service, we directly consent to what a company does with our data. This is different from consent for government data collection. Wisnewski states that citizens consent through the democratic process (Wisnewski 2016, 210). Citizens consent to state surveillance by re-electing the government that put the surveillance in place. Wisnewski notes that there needs to be informed consent by citizens of a state but that there is a balance between being informed and demonstrably blocking state action by requiring total consent by citizens. Citizens need to know they are being monitored digitally, but not exactly how or what is being monitored (Wisnewski 2016, 211). To this end, Wisnewski notes that when it was revealed that the state conducted mass surveillance on its citizens, as in the Snowden leaks, the response was relatively apathy; this apathy does not make mass surveillance right but nonetheless legitimizes it. Arguably, this apathy allows governments to expand mass surveillance even in cases in which the secret programs are revealed through leaks or other means. As shown in the Snowden leaks, the mass surveillance programs of the NSA were well covered in the media and caused some protests by the public but did not result in any tangible and public changes to the mass surveillance apparatus. Instead, the NSA has continued to expand its capabilities to process vast amounts of data, as shown by the construction of the NSA data center in Utah, which is projected to have the ability to hold exabytes[6] of data. The apathy that Wisnewski discusses is tangible every time the NSA or Five Eyes is in the media cycle or brought to the public attention, and little is done to reduce surveillance expansion.

In contrast, Bannister weighs the risk to privacy for the individual and the community. Bannister argues that citizens often trade privacy rights to protect the security of the community. However, there is a risk to allowing small concessions, such as the need to take fingerprints when crossing borders, because these small infractions can coalesce into a considerable reduction of privacy rights (Bannister 2005, 76). Furthermore, Bannister argues that legislation that impacts a person's

[6] An exabyte is one billion gigabytes. In comparison, the average smartphone has a storage capacity of 128 to 500 gigabytes.

privacy is usually made in response to a horrible event such as a terrorist attack, making laws that sacrifice privacy for security messy and rushed. Again, Bannister argues that rights, like privacy, need to be traded, to an extent, for some collective security. In Bannisters' view, laws impacting privacy must have four requirements to ensure that changes are prudent. First, a body with collective expertise should be established to judge if there is a balance between what should be permissible and what lines should be drawn. Second, all anti-privacy legislation must be temporary. Third, there should be regular independent reviews of how the state uses personal information. Lastly, Bannister calls for public debate on balancing individual and community risks.

There is also the question of what role or value intelligence provides to the state. The relationship between intelligence and democracies in the literature describes intelligence as a "product" for the government, akin to how fiscal reports by the Department of Finance are products for the government to aid in decision-making (Matei and Halladay 2019, 1). However, there is a paradox in the relationship between intelligence agencies and democracies. On the one hand, to protect the rights and transparency of democracies, so the argument goes, intelligence agencies need to act covertly and in secret. It can be argued that intelligence and security agencies protect the state and its mechanisms, such as the democratic process, from threats like foreign interference. To do so, they must operate in secrecy to prevent threat actors from changing their methods to evade detection. On the other hand, the need for secrecy in intelligence agencies leads to the risk of abuse of power by said agencies. This risk is exacerbated by a lack of oversight bodies to keep intelligence agencies in check. Canada, for example, did not have an intelligence oversight framework until 1984 as a result of the McDonald Commission[7] (Matei and Halladay 2019, 2, Leigh and Wegge 2019, 154). This lack of oversight can lead to the abuse of power that transformed the RCMP Security Service into the Canadian Security Intelligence Service after the McDonald Commission. The purpose of intelligence oversight in Canada is documented in the *A New Review Mechanism for the RCMP's National Security Activities* produced by Justice O'Connor as part of the Maher Arar Commission. In this report, O'Conner states that intelligence oversight and review must ensure the following: assurance of conformity with the law, foster

[7] The McDonald Commission or the *Royal Commission of Inquiry into Certain Activities of the RCMP* was a commission into the illegal activities by the RCMP Security Service, CSIS's predecessor. The actions investigated included illegal break ins and illegal wiretaps. The commission resulted in the creation of CSIS and the transfer of the domestic intelligence mandate of the RCMP to CSIS.

accountability to government, foster accountability to the public and facilitate public trust and confidence, and not impair national security (2006, 464-472).

People experience privacy and state security differently. States categorize people, both citizens and non-citizens, into groupings that the state views as requiring more of less surveillance due to the perceived threat they pose. Importantly, the impact of increased surveillance can lead to less security for those perceived as threats. There are several examples of privacy violations and security measures used on people due to agency perceptions of threat. The 2010 Winter Olympics in Vancouver, for example, showcased the state changing surveillance targets based on a changing view on security threats. At first, the joint intelligence centers set up to protect the 2010 Winter Olympics focused on terror groups such as Al-Qaeda targeting event infrastructure (Monaghan and Walby 2012, 141). However, the focus of state protection shifted to protecting the corporate sponsors of the event and targeting groups protesting the games, often focusing on left-leaning groups (Monaghan and Walby 2012, 144). This shift meant that the state targetted groups exercising their democratically protected rights to protest the games, including CSIS conducting surveillance operations on several activists (Monaghan and Walby 2012, 137, 141). The state went from protecting the games from "the other" to targeting those within, devoting resources to surveilling, thus violating the rights and privacy, of different groups. Who the state views as a threat often shifts as exogenous factors change, in turn, those who become new threats experience privacy differently.

3.4 Conclusion

In this chapter, it is clear that research differs on what privacy is and its relationship with national security. Also, while the research on CSE itself is limited, past research into the agency has revealed that CSE has spied on Canadians before, and the legal framework to support CSE's activities has become more permissible over time. Furthermore, past research into CSE via the Snowden leaks and other CSE documents shows that CSE's capabilities are sophisticated and enhanced by the Five Eyes alliance.

In the next chapter, the idea of privacy and security will be explored. It will use the literature on privacy in this chapter to develop a theory of privacy used for the analysis of whether CSE impacts Canadians' privacy and, if so, to what extent.

4. The Ethics of Privacy and Just Surveillance

Exploring the question of whether CSE violates Canadians' privacy must be prefaced by an understanding of what privacy means. Although some of the literature related to privacy, intelligence and the state was reviewed in Chapter 3, this chapter delves into theories of privacy more deeply. Much of the scholarship on privacy focuses on surveillance and not the theoretical aspects of privacy in the digital age. There is also little research into the theoretical aspects of privacy in an era of mass surveillance. In this chapter, I will merge previous literature on the theoretical concepts of privacy and literature on mass surveillance and privacy. An understanding of how CSE impacts Canadians' privacy beyond the legal definition will be employed to further my analysis.

4.1 What is Privacy?

As explored in the literature review, the definition of privacy is complex. This chapter aims to define privacy further. In his book *Windows into the Soul*, Marx (2016) states that privacy is "… a multidimensional concept with fluid and often ill-defined, contested, and negotiated contours dependent on the context and culture" (27). Privacy involves many aspects of the self, including information. This thesis uses informational privacy as its subject. However, informational privacy itself is an unsettled subject. Many scholars, states, and international organizations have differing views on privacy.

In *National Security, Personal Privacy and the Law*, Sharpe (2020, p.1) states that privacy is considered by most to be a negative liberty of not having the state coerce a person into revealing personal information (1). Furthermore, Sharpe identifies three areas in which laws have been identified as private. First is the right for behaviour in a private space to be private. Second is the right not to be eavesdropped upon. Third is the right not to be known about. However, Sharpe notes that in the current digital and globalized world, it is difficult to sustain these rights (Sharpe 2020, 2). Similarly, Stalla-Bourdillon (2014) argues, from a legal perspective, that privacy is the "right to let alone," as coined by Warren and Brandis (8). In other words, it is the right to a public and private life. In a similar definition, Watts (2021) argues that privacy is the presumption of an area in a person's life free from the state and excessive unsolicited intrusion by other uninvited individuals (14). All of these ideas coalesce around the idea that privacy is a negative freedom.

In contrast, Miller and Walsh argue that it is a moral right of a person to control information about themselves (2016, 195). Sloan and Warner also use this definition of privacy (2016, 370). Privacy is a boundary of making ourselves available to others, be it information, time, space, etc. (Sloan and Warner 2016, 370-371). Privacy is the ability to control personal information, allowing a person to choose what they reveal about themselves to whom. When a person loses this control, they lose their privacy. Here, privacy is conceived of as a right to present oneself as one chooses and thus carries with it some sense of privacy as a positive liberty (however minimal).

From the above definitions of privacy, several themes and differences are present. One view of privacy is that privacy is based on how the individual controls their information. A person can control the information present in both their private and public life or that they have control over how information is distributed and to whom. Another view involves the state and how much it is present in a person's private life. These definitions provide a clear boundary of what is private and how information can be private. However, they lack clarity when applied to the digital context.

With differing understandings of privacy, the question of what privacy is remains. Legally, the Canadian government determines privacy based on personal information defined in the *Privacy Act*. However, a purely legal lens of privacy is extremely limited. The *Privacy Act* limits personal information to information on who the person is, such as race or employment history (Privacy Act 1985). Additionally, the *Privacy Act* treats personal opinions and viewpoints as personal information.

Ethical and moral considerations must also be considered when looking at the impact of mass surveillance on privacy. A purely legal review of privacy would be limited in the context of this thesis. For example, the *Communications Security Establishment Act* forbids CSE to collect Canadian information that "…interferes with the reasonable expectation of privacy…" (Communications Security Establishment Act 2019). However, this same section states that ministerial authorizations can overturn the restriction. This is an example of one of the many different privacy restrictions on CSE that retain a legal mechanism to be dismissed.

In order to analyze how CSE impacts Canadians' privacy, this thesis will use the understanding that privacy is the ability of individuals to control personal information. When people lose

control of personal information without their consent, their privacy is violated. This understanding was chosen as it covers the need for a person to consent to have their personal shared with a third party. This consent is vital in the digital age as information is shared by third parties every day, from social media to targeted advertisement. It is when this information is captured or shared without consent that privacy is violated.

4.2 Privacy and the State

The relationship between a person's privacy and the state is complex. First, there is the distinction between the citizen and the non-citizen. In the Canadian context, citizens and permanent residents[8] enjoy protection from specific government actions via constitutional protections. Non-citizens do not. That being said, under Canadian law, the Canadian state can not be complicit in actions that cause harm to persons or democracy, even if they are non-citizens. However, non-citizens are not offered the same level of protection from government actions. This distinction is why there are no limits on the actions of CSE towards non-citizens.[9]

The relationship between the citizen and state when it comes to privacy is often expressed in terms of finding the appropriate "balance" between liberty and security. For example, there is a balance between the state's security and its citizens' autonomy. Nevertheless, citizens have both a right to privacy and a right to security or public security (Stalla-Bourdillon, Phillips and Ryan 2014, 67). Exercises of national security are defended as legitimate ways to ensure citizens have security, as protecting national security is claimed to be about protecting not only the government but also the citizenry from injury. However, national security does not fully overlap with public security. As such, the state needs to balance protecting itself and its citizens while protecting citizens' other rights. However, this relationship has become a complex balance in the digital age. A citizen can argue that they can encrypt their communications as they are private. The state can argue that it needs access to encrypted communications to prevent possible crimes and actions that would harm the state and its citizens. This leads to citizens' privacy rights being eroded in the name of national security and public safety.

The erosion of citizens' privacy can have negative consequences for the citizens. Sloan and Warner (2016, 381) argue that a lack of privacy in public harms the realization of the self. Their

[8] And to a point, people within Canadian borders.
[9] And foreign intelligence agencies in general.

argument is unique in exploring the philosophical impact of surveillance by the state on the self. Privacy in public is the control of information that informs how others view you. It is also the ability to control how much people know about you. Sloan and Warner argue that part of wanting privacy in public is to avoid disapproval and reprisal from others in a community (2016, 370). Furthermore, controlling the information known by others about oneself is a means of defining one's role and place in society. As such, controlling personal information, especially that which is known by the state, is a key part of this control. The state of knowing information about a person has a chilling effect that impacts how they can define their roles in society (Sloan and Warner 2016, 384). Sloan and Warner (2016, 384) argue that the idea that the government "merely knows" information has a chilling effect, as what the government knows about us defines how we appear to the government. How we appear to the government impacts how the government interacts with us. One's appearance to the government could impact any or all aspects of state interaction with us. A mundane person to the government likely means they will have mundane interactions, while a person known to the government to falsify their taxes would face additional scrutiny by the state tax agency. How one appears to the government also impacts democratic rights, such as freedom of expression.

For example, a political dissenter or protester may limit their expression of public dissatisfaction about government actions if they know the state collects their information *en masse*. Thus, the government is guaranteed to know of their public dissatisfaction and being labelled as a dissenter. Furthermore, knowing the state knows one's associations also influences how one conducts themselves. The state's knowledge of said relationship may, in fact, turn a two-party relationship into a three-party relationship: one between the person, the organization, and the state. This influences how a person conducts themselves as the relationship is no longer the original two-party relationship but a three-party relationship with an unwelcome party, the state.

4.3 Intelligence, Digital Information, and Privacy

When the state collects intelligence, especially SIGINT, the resources needed for the state to disrupt a person's privacy are trivial for the amount of information gathered. Furthermore, intelligence and mass information collection are simply tools that the state can use to gather information on its citizens and non-citizens. The collection of information via SIGINT or digital in general is now invisible, meaning the target cannot observe the collection of information. In

other words, unless the target is highly knowledgeable or knows they are a target, it is impossible for them to know they are being surveilled. In the past, the state needed to conduct physical surveillance or, at the very least, physically tap phone lines. The classic visage of a man sitting on a bench looking through holes in a newspaper is no longer the case. Furthermore, states and actors were previously limited in scale due to the resource-intensive nature of physical surveillance (Marx 2016, 17). However, the previous limits of scale, time and resources needed for surveillance are no longer restrictive. The state can surveil with relative ease, and surveillance is only increasing in ease as technology develops. This ease is illustrated further below.

Currently, it is almost impossible for a person to know they are being surveilled. It is this unknown quantity which impacts a person's privacy. As such, the unknown can make a person see the state as a bad actor. When a person's information is collected by an entity, such as a state, they have no control over how that information is used. In the case of the state, especially with secretive intelligence agencies, a person has no idea or understanding of what information the state has nor how it is being used. People, in general, do not approve of being spied upon or surveilled. This leads to the perception that information gathered can be harmful or cast suspicion, and rightfully so. The state is a powerful entity, more so than a corporation could be. Governments have used personal information to discourage and prevent behaviour they do not agree with (Sloan and Warner 2016, 380). Governments can use information against those they deem undesirable, such as dissidents or journalists. While corporations, especially large ones, can use information against those they see as undesirable, they are limited by the laws of the state. The state, in theory, can adjust its law to remove any restriction on surveillance.[10] Thus, it is easy to assume for a person that the state will use their information against them as they can be deemed "undesirable" by the state, which could theoretically be done at any time for any reason.

However, the characterization of the state as a bad actor only occurs if a person knows that the state is conducting surveillance. For example, while there were concerns about mass surveillance by the US prior to the Snowden leaks, it did not reach mainstream concern until the public was made aware of the mass surveillance programs. Thus, when the mass surveillance programs were

[10] This argument of course varies state by state. A totalitarian state can easily remove restrictions verses a state with more checks and balances on state power.

made public, the majority of the reaction was negative (Connor and Doan 2019, 58). People widely viewed the violation of privacy by the state as threatening. They saw the level of information collection as an unjustified means of protecting national security.

In contrast, others saw mass surveillance as justified as they deemed national security to supplant concerns with personal privacy (Connor and Doan 2019, 59-60). However, many were still concerned with how much the state could collect about a person's life with relative ease. This unknown but presumably voluminous quantity of data arguably amplified the fears that the state was using their information for malicious purposes.

With the vast volume of information governments can gather, the question is whether the government is using it for some defined purpose or simply collecting it. Aside from the argument on whether the state *should* be collecting such vast amounts of information on citizens, there is a distinctive question about the *impact* on a person's privacy if the information is used or even accessed. If the information of a person's phone call sits on a server with no one to look at it, is it a violation of a person's privacy? On one side of this argument, the very exercise of state power to use this information produces a violation of a person's privacy. Tools such as XKEYSCORE mean that vast amounts of personal information are available to an analyst with a single XKEYSCORE query. However, most of the information gathered by agencies like the NSA and CSE is automated. Mass surveillance is not an active process but rather a passive one (Gill and Phythian 2018, 85-86). Much of the data gathered through programs like PRISM sits on servers waiting to be accessed (Gill and Phythian 2018, 85). However, it is relatively easy for a person to come to the attention of intelligence agencies. A common practice known as "contact chaining" uses the connections of targets to find other possible persons of interest (British Columbia Civil Liberties Association 2023). Contact chaining is a catch-all process. As a result, there is a chance that knowing a target or contacting someone who contacted a target makes you one. Thus, the passive collection of data is not intrinsically benign.

Mills (2016) provides a hypothetical scenario that highlights the ease with which incidental connections can cause a person's information to be targeted and processed by the NSA. In his scenario, Jane Doe messages a person who is connected to a possible terrorist target. By doing

so, Jane becomes a third contact in a chain.[11] Jane's location is recorded by the GPS on her phone. Her Gmail and Facebook photos are collected through PRISM. Her telecom provider has already provided her call logs. An interested analyst can then review her Google searches of the past five years through XKEYSCORE (2015, 221). This example illustrates the ease of collection and amount of information available to modern intelligence services. The purpose of including this example is to show how citizen privacy can be "intruded" on in the modern day. Part of the issue is that bulk collection is primarily an automatic process providing a gateway to enrolling in a chain for deeper surveillance.

Additionally, and as mentioned above, the collection of digital information by states is an invisible process. While citizens know that bulk information is being collected, they do not know how personal information is collected. Let us return to Sloan and Warner's understanding of how knowing personal information is collected influences citizens' actions. If someone does not know their information is being collected, they will not change their actions. This makes covert surveillance vital to the state's ability to collect information. However, this also means that it is almost impossible for a person to directly consent to, let alone challenge or avoid, mass surveillance.

Like any surveillance, there are degrees of intrusion. Just as following someone is arguably less intrusive than having hidden cameras in their home, digital surveillance differs in scale. There is an arguable difference in the collection of metadata and targeted content collection as surveillance techniques vary in scale and impact. For example, collecting one person's metadata has a relatively small privacy impact as it collects information that a communication was sent rather than what was in said communication.

However, at the scale collected by intelligence agencies and companies such as Google and Facebook, the privacy impact is vastly increased. The scale on which intelligence agencies and companies can surveil people has vastly increased. The NSA collects vast amounts of information every single day. The Snowden leaks show that the NSA collected data on 97 billion emails and 124 billion phone calls in one month in 2013 (Greenwald 2014, 92). This vast amount

[11] Contact chaining is an analysis process where a targets social links is targeted. Those new targets social links are added to the surveillance. This is used to identify other possible targets. In other words, a suspected terrorist texts a friend, then whoever that person contacts becomes a target.

of covert information collection impacts a similarly vast amount of people. At the same time, each individual collection of data is arguably small, such as knowing who sent an email to whom; each individual collection assembles into a process that impacts the privacy of millions of people.

4.4 Is Surveillance Ethical?

It should be noted that ease of surveillance is neither an inherently harmful prospect nor the idea of surveillance itself. The ethical/moral question of surveillance is one of debate, and to adequately address the issue would require a thesis in itself. However, it should be discussed to provide moral context to the topic of this thesis. The discussion of SIGINT in Chapter 2 illustrates ease of access. It can be argued that ease of access benefits both the state and its citizens as it is a means for the state to protect itself and its citizens from malign actors. While surveillance is often vilified, many claim it plays a vital role in state security. Several scholars have theorized that surveillance can be just when the proper requirements are met.

Allen (2016) argues that surveillance can be justified but depends on the situation and subject. At the state level, Allen uses the increased surveillance in response to the War on Terror during the Bush administration as her example. She notes that the Bush administration used the protecting national security/war on terror rationale to justify the sidelining of the *Foreign Intelligence Surveillance Act* (FISA) court process and other government surveillance restrictions by executive order. The Bush administration lost the political battle regarding warrantless surveillance. As a result, the Bush administration conceded to obtaining warrants for its surveillance (Allen 2008, 18). The situation did not warrant a vast surveillance network without legal backing. This made the surveillance unjustified in the eyes of the citizens. However, it is not to say that the War on Terror does not justify any surveillance. Rather, it only justifies surveillance to a legally circumscribed extent.

Macnish (2014) explores the idea of just surveillance using the theory of just war. Macnish argues that the philosophical analysis is currently disjointed and lacking, finding many analyses lacking and not covering the important aspects of war and surveillance and their interconnections (2014, 146). As such, the established theories of just war can be used to study what just surveillance should look like. Macnish proposes seven principles of just war that integrate with

the concept of just surveillance, of which there are several of note. The first principle is "just cause" for surveillance.

The justifiable cause varies for each situation or actor. However, for the state, public safety is the purported basis for justifiable surveillance. Just as the state may conduct war to protect itself and its citizens, it can conduct surveillance to protect itself and its citizens from threats that may lead to war (Macnish 2014, 148). However, if a state were to conduct surveillance on political dissidents or marginalized groups without evidence to demonstrate that they present a legitimate security threat, it would be an arguably unjust cause. However, Macnish makes the caveat that while the reasoning for the surveillance may be just, it may not justify the surveillance in its totality. The second principle links into the first, as there must be "just intention." As with just war, the intention of the surveillance must be just. If surveillance is conducted with ulterior motives rather than the proposed just cause, the surveillance cannot be just. For example, if a state were to justify surveillance to combat a terrorist threat but were to focus on political dissidence, it would not be adhering to just intent. The third principle depends on who is conducting surveillance and on whose behalf. For example, if the state were conducting surveillance on behalf of the protection of its citizens who face a serious threat, it would be just.

Although Macnish acknowledges that some principles of just war do not fit with a theory of just surveillance due to its covert nature, they nevertheless theorize two modified principles that can justify the means of surveillance. The first is the principle of proportionality. Macnish argues that the less extreme the situation, the less intrusive the surveillance response should be. He gives an example of CCTV being used to monitor high-crime areas in contrast to wiretapping all the phones in the area (Macnish 2014, 151). In other words, it may be reasonable and just if the state uses its surveillance capabilities to gain information on an area rather than resort to monitoring the phones of all the people who reside there, which would be disproportionate because securing space is less intrusive than monitoring personal communication devices. The second surveillance-specific principle is the distinction between legitimate and illegitimate surveillance targets. Macnish notes that there is a difficulty with this principle as a target of surveillance often needs to be watched to determine if it is a legitimate target. As such, Macnish argues that pre-existing evidence must be used to determine if a target is legitimate. This reduces the possibility that an illegitimate subject would be targeted.

With this understanding, can surveillance be ethical? I take the position that, yes, surveillance can be ethical if it is used by the state to protect itself and its citizens from legitimate threats. However, just surveillance comes with the caveats that it must be focused and not break the legal restrictions that the state has placed upon itself through democratic and constitutional processes and principles. These restrictions include legal restrictions and judicial and quasi-judicial rulings, such as those from oversight bodies. It must be proportionate to the end the surveillance is trying to achieve.

4.5 Conclusion

Using the definition of privacy and the understanding that surveillance can be just, the thesis will analyze whether CSE is interfering with Canadians' privacy, as well as consider whether its use of information is just. However, to do this analysis, what CSE is using Canadian information for and how it is used must be understood. How CSE collects and uses Canadian information is explored in the next chapter.

5. Findings and Research

For this thesis, I collected several types of documents for analysis. All documents were collected from Access to Information requests or publicly available documents. Any documents with classification markings were released through ATIP.

There are also caveats in the analysis pertaining to the dates of government documents used for research in this thesis. The documents used for analysis are from before and after the passing of the *CSE Act* (2019). Some documents and reports are from CSE's mandate when it was within the *National Defense Act.* The thesis uses pre-CSE act documents to provide more information in its analysis as reports and documentation available to the public post-CSE Act are very limited as the change is relatively new. An additional caveat is that using information with redactions or missing information, in general, makes it impossible to be fully confident with analysis. Much of the analysis in this chapter and the next is conjectured based on the information available. However, with enough information from the sources used in this thesis, an understanding of CSE's policies and procedures can be found. Also, as noted in the Introduction of the thesis, I have triangulated some documents in order to glean more information upon which to base my analysis.

This chapter is organized around three themes relating to three types of documents under analysis: Legal, Policy, and Reviews. Legal documents relate to the legal aspects of CSE's mandate. Policy documents include any policies, procedures, or instruction documents created by CSE. Review documents include reviews and assessments by oversight and review bodies of CSE. These three themes reveal how CSE manages its legal obligations to Canadian privacy, its processes, and its shortcomings in doing so.

5.1 Legal Themes CSE's Mandates under the CSE Act

Under the Communications Security Establishment Act, CSE currently has five separate mandates: foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations, and operational assistance *(Communications Security Establishment Act*, 2019, 7). Before 2019, when CSE was under the *National Defense Act*, it had three mandates: foreign intelligence, cybersecurity, and operational assistance. Before the

passing of the CSE act, the three mandates were referred to as mandate (a), mandate (b), and mandate (c), respectively. Regarding Canadian information, CSE has clear restrictions on its ability to target and collect Canadian information. Section 22 of the CSE Act states:

> Activities carried out by the Establishment in furtherance of the foreign intelligence, cybersecurity and information assurance, defensive cyber operations or active cyber operations aspects of its mandate must not be directed at a Canadian or at any person in Canada and must not infringe the *Canadian Charter of Rights and Freedoms* (*Communications Security Establishment Act*, 2019, 9).

However, the *CSE Act* allows CSE to collect Canadian information "incidentally." Section 23 (4) of the *CSE Act* states that: "The Establishment may acquire information relating to a Canadian or a person in Canada incidentally in the course of carrying out activities under an authorization issued under subsection 26(1), 27(1) or (2) or 40(1)" (Communications Security Establishment Act 2019, 10).

The *CSE Act* states that the CSE must take measures to protect the privacy of Canadian information in the "… use, analysis, retention and disclosure..." of Canadian information collected in its foreign intelligence, cybersecurity and information assurance mandate. Furthermore, the Act also codifies that CSE, when acting under its operational assistance mandate, "… has the same authority to carry out any activity as would have the federal law enforcement or security agency…" (Communications Security Establishment Act 2019, 11).

The *CSE Act* also allows CSE to disclose Canadian information to other departments of the Government of Canada. Section 43 of the Act states that CSE may disclose any information that could be used to identify a Canadian or person in Canada if CSE concludes that the disclosure is "…essential to international affairs, defence, security, or cybersecurity" (Communications Security Establishment Act 2019, 21).

5.2 Policy

Most of the information on how CSE collects, handles, and shares Canadian information is in CSE's internal policies. Many of the policies are from before the creation of the *CSE Act*. As such, they may be outdated and do not include any of the new mandates. However, I contend that these policies still provide information on how CSE operated around the time of the document's

publication date, 2017, and analysis of them can still provide valuable insight and information on CSE policy approach to the collection and use of Canadian information. An updated SIGINT policy suite, now titled *Mission Policy Suite*[1], was requested but was not received in time for inclusion into this thesis. Consequently, many of the policies used for research reflect the foreign intelligence mandate, not the cybersecurity and operational assistance mandates.

5.2.1 SIGINT

CSE has several operational procedures intended to address how to use Canadian information and ensure privacy is respected. These operational procedures reveal what CSE views as Canadian information and how it is obtained (again, prior to the passing of the *CSE Act).* The procedure *OPS-1-7: Operational Procedures for Naming in SIGINT Reports* specifically mentions Canadian and Second Party identities. It defines a Canadian as a Canadian citizen or a permanent resident of Canada (2012, 6). However, persons in Canada under a student, worker or visitor visa can be named but not targeted if they are in Canada. It defines identity as uniquely associated, directly or indirectly, with Canadian residency, if not citizenship (2012, 7). It gives several examples of such information: " a name, [REDACTED] telephone number, e-mail address, IP address, passport number [REDACTED]" (Communications Security Establishment Canada 2012, 7). The document also states that the analyst must suppress the Canadian identity. They must use a generic referral to the identity. The procedure uses "a Canadian company" and "a Canadian person" as examples. However, the procedure guides an analyst in naming a Canadian in a report. For example, a Canadian can be named if they work for an international organization when acting in their official capacity. They can name the title of the Canadian or directly name them if it represents foreign intelligence value (Communications Security Establishment Canada 2012, 13). Other situations or who the person is can lead to Canadian information being released unsurpassed. These include federal ministers acting in their official capacity, Canadians working at the United Nations, and in their official capacity if it is necessary to assess its importance. However, the analyst cannot indicate that the person is Canadian. An interesting requirement is regarding Canadian cities and provinces. An analyst can only name city or province when using them for geographic reference but must be generic when referring to the "…identities or the political, social or economic agendas of municipal, provincial or

[1] This name was given to me in a request for further information by CSE when I requested the updated version of the OPS policy suite.

territorial people, corporation or organizations may be revealed" (Communications Security Establishment Canada 2012, 14) . Some examples are fully redacted, and the section on naming e-mails and IP addresses is fully redacted except for mentioning e-mail addresses and IP addresses. From these details, it is reasonable to conclude that as long as the Canadian information relates to the Government of Canada, a high-level government official, relates to a foreign government, or is used as a location reference, it can be released unsuppressed in CSE SIGINT reports.

However, many situations outside the procedure's examples need approval from CSE's oversight division. The policy also provides explicit rules on sharing Canadian identities. The "Release and Retention of Identities" section explicitly states that only essential details of an identity are to be used. Furthermore, it states that only the Operational Policy section of CSE can release unsuppressed identities. The example in this section gives insight into how focused the policy is on controlling the release of unsuppressed Canadian information. The example reads: " This means, for example, that you must never provide a Canadian or Second Party identity to a CSIS analyst, by any means, including by telephone (Communications Security Establishment Canada 2012, 11)." From this section, it is clear that CSE is very controlling of who can receive Canadian identities.

The heavily redacted "Naming Canadians [REDACTED]" section provides little insight. The context of the section is unknown, the only non-redacted text being: "It is not unusual to find a Canadian, usually with dual citizenship, [REDACTED]. Although such a Canadian is considered to be [REDACTED] privacy protections still apply" (Communications Security Establishment Canada 2012, 28). The procedure also discusses how to prevent the identification of a person via context, e.g., if a Canadian can be identified via the report's context if an informed person were to read it. This procedure shows many variables to consider when using and naming Canadian information in CSE's SIGINT mandate. However, most of the variables are redacted. The variables focus on removing the information that identifies the person as Canadian. For example, the analyst must not indicate that the person is Canadian or is a permeant resident. There is also a point that might cover if a Canadian was previously named. It states: "If and when this Canadian person [REDACTED], you must stop naming him or her, and must not footnote reports that did name this person" (Communications Security Establishment Canada 2012, 29).

Canadian naming examples are given in Annex 2. This annex clarifies the distinctions of what is "Canadian." For example, a Canadian citizen should be written as "a Canadian citizen," but an honorary Canadian citizen can be named. Foreigners within Canada can also be named, including those under special visas. The annex gives student or work visas as examples. This goes directly against the prohibition of CSE's activities on persons in Canada. While this prohibition does not apply to the operational assistance mandate, there is no distinction or direction on the protections of non-Canadians living in Canada under this prohibition. If such information is present, it is redacted. This makes it unknown what privacy protections there are for foreigners within Canada, and at worse, it means CSE is not following its legal restrictions.

The operational procedure, *OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*, provides insight into how CSE interacts with Canadian information. The procedure states that if a Canadian or person in Canada is inadvertently targeted, the selector used must be de-targeted,[2] any existing traffic from the selector destroyed, any SIGINT Reports based on the traffic cancelled, and the oversight and compliance section notified (Communications Security Establishment Canada 2012, 7). Furthermore, the procedure states that analysts who recognize private communications of Canadians, communications of a Canadian outside of Canada, or about Canadians and do not provide foreign intelligence value[3] must mark the traffic for deletion. However, if Canadians' communications outside of Canada are deemed to have foreign intelligence value, privacy annotations must be marked. These annotations will be explored further in this chapter.

The policy also has a section regarding the authority to intercept under section 16 of the *CSIS Act*. However, this section is wholly redacted and marked as IRRELEVENT.[4] Since this area is entirely redacted, it is impossible to know the additional legal context and guidance the policy provides regarding CSE's assistance to CSIS. However, the fact that it has a specific section hints that SIGINT interceptions on behalf of CSIS are very common.

[2] A selector is a characteristic of a targeted person or a device of a person, e.g., email address, phone number, IMEI, etc. De-targeting means information about the selector is no longer captured.

[3] The procedure specifically states "essential to international affairs, defence or security"

[4] This source was taken from a original ATIP request from the BC Civil Liberties Association. As it is not an original request made by myself, the sections on CSIS authorities may not have been covered in the request by the BCCLA.

This policy clearly shows that CSE has detailed policies regarding collecting and handling Canadian information. Additionally, it reveals that CSE routinely collects and handles Canadian information. This revelation is further confirmed by the existence of several policies regarding the collection of Canadian information. This fact directly conflicts with CSE's prohibition on directing its activities on Canadians. Further, the policy even states that CSE collects, handles, and stores Canadian information. When taken at face value, CSE collecting and storing Canadian information directly conflicts with its prohibition on collecting Canadian information. Other sources address this conflict, such as a backgrounder in a CSE Commissioner report stating that CSE retains "unintentionally" collected Canadian information (Office of the Communications Security Establishment Commissioner 2019, 10). This practice may comply with the law but arguably goes against the spirit of the prohibition.

CSE releases suppressed Canadian information to specific entities. The procedure *OPS-1-1: Operational Procedures for the Release of Suppressed Information from SIGINT Reports* lists the following parties who can request Canadian information: Government of Canada "clients," CSE staff, Second Party government personnel via SIGINT policy offices, and CSEC Client Relations Officers.[5] The procedure lists several conditions the requester must meet before releasing Canadian information. The conditions are: the information requested must be within the department's mandate, the released information is under the control of the receiving agency, and if the requesting department is in Canada, it will handle information in accordance with the *Access to Information Act* and the *Privacy Act* (2012, 9). The requester must also give a rationale for requesting Canadian Information. The procedure states that at least one of the given rationales must be met. However, most example rationales are redacted and, therefore, impossible to investigate. The redactions in the procedure cover all but three possible rationales:

> Capabilities/intentions/activities of a foreign person, state, organization or terrorist group relating to international affairs, defence or security, and use for prevention/identification/investigation of a potential threat to the life or safety of an individual in Canada or abroad (2012, 10).

[5] CSE Client Relations Officers are liaison officers to Government of Canadian departments.

From this section, it seems that there needs to be a national security justification from the requesting department for it to receive Canadian information. However, there may be other types of justifications that are redacted. For example, other justifications could pertain to an RCMP or CSIS investigation. This leads to more questions on the use and availability of unsuppressed Canadian information to other government departments. Unsuppressed Canadian information is very sensitive as it links people directly to the SIGINT gathered and has a massive impact on their privacy. Not knowing the reasons for sharing such information leads to questions of whether it is being shared or appropriately handled and if it should be shared at all.

Additionally, the OPS-1-1 procedures reveal how CSE stores Canadian information. After an analyst suppresses a Canadian identity, they enter it into a repository for suppressed information. Only the Operational Policy staff and analysts can access the unsuppressed information. Only if a suppressed Canadian Identity is requested and approved for dissemination for the above reasons is it shared outside CSE.

Furthermore, the document *CSOI-5-8: Active Monitoring Procedures for [REDACTED]* from 2009 shows the management process of target selection. While most of the title is redacted, the objective of the procedure manual states:

> These instructions outline the procedures that apply to the [REDACTED] in establishing and implementing an active monitoring program for SIGINT systems and processes within their area of responsibility (Communications Security Establishment Canada 2009, 4).

Section 2 of the procedure outlines validation checks collection managers must perform before enacting targeting requests. All new targeting requests must validate that they include appropriate justification, meet valid Government of Canada requirements, adhere to SIGINT priorities, comply with policy and legal constraints and technical feasibility, and ensure the SIGINT system is not jeopardized. Furthermore, the collection managers must confirm that CSE targeting requests are directed at a ***foreign*** entity located ***outside*** of Canada (emphasis in original text) (Communications Security Establishment Canada 2009, 9). This procedure document does not outline or give examples of appropriate justification. It likely relates to other requirements, such as government intelligence priorities or legal justification, such as under CSE's foreign

intelligence mandate or by CSIS under the *CSIS Act*. However, there is no clear definition of what “appropriate justification" means, so there is no definitive answer.

The SIGINT working aid titled *Foreign Assessments and Protected Entities* guides analysts when determining if a target is foreign. If an analyst is unsure if a target is foreign, they are to use the least intrusive forms of research. The working aid suggests using the Target Knowledge Database, the report dissemination tool or non-SIGINT sources. While there is no direct description of the Target Knowledge Database from the name, it is likely the database used by CSE to hold all information or descriptors of SIGINT targets. It is unknown what the size or information retention period is. When combined with information from other policy documents, the different types of selectors common in SIGINT are likely stored and linked to targets, such as phone numbers, IP addresses, and other personal information.

It also recommends consulting with other agencies, such as the CBSA. Analysts are to use CSE’s metadata databases if these sources do not provide clarity. Furthermore, if Canadian-related information is connected to the target, the analysts' manager must pre-authorize any use of SIGINT information before it can be used to determine if a target is foreign (Communications Security Establishment 2014, 2). Figure 1 below shows this guidance section.

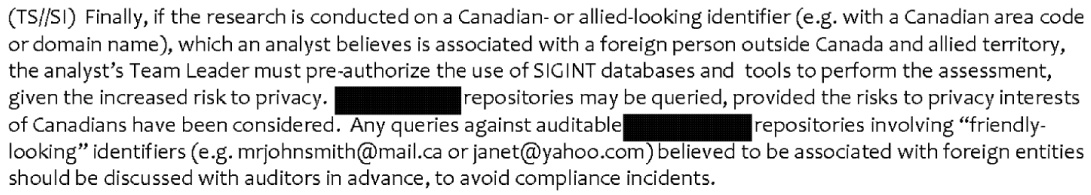

(TS//SI) Finally, if the research is conducted on a Canadian- or allied-looking identifier (e.g. with a Canadian area code or domain name), which an analyst believes is associated with a foreign person outside Canada and allied territory, the analyst’s Team Leader must pre-authorize the use of SIGINT databases and tools to perform the assessment, given the increased risk to privacy. [redacted] repositories may be queried, provided the risks to privacy interests of Canadians have been considered. Any queries against auditable [redacted] repositories involving “friendly-looking” identifiers (e.g. mrjohnsmith@mail.ca or janet@yahoo.com) believed to be associated with foreign entities should be discussed with auditors in advance, to avoid compliance incidents.

Figure 1. Guidance on Canadian or Allied Looking Identifiers

Many issues and questions arise from this guidance section. The initial assessment of a target that is Canadian seems based on the analyst's beliefs. This process can lead to varying privacy impacts depending on how an analyst “feels” about a target. There is also the question of what “friendly looking” means in this context. The types of repositories for “friendly looking” identifiers are unknown due to redactions but could mean protected or repositories of second-party identifiers. Likely the same repositories containing the “protected” information discussed below. Much of this process is up to the beliefs of the analyst, who likely have their own bias and

ideas of what is “friendly looking.” Without official definitions of " friendly looking, " the initial privacy impact of determining if a target is Canadian varies by CSE analyst, which is concerning.

The repositories used in this procedure are auditable, recording any access and usage. If a target is found to be Canadian or “allied,” the analyst needs to mark it as “Protected” in the CSE Target Knowledge Database (Communications Security Establishment 2014, 3). The working aid states that this will prevent further inadvertent targeting or privacy incidences related to the target. The working aid also notes that marking entities of intelligence interest with clear links to Canadian or allied identifiers, marking such entities as “Protected,” has received positive feedback from CSE’s oversight agency. The working aid guides how much information should be included when marking a target as “Protected” to link the Canadian identifier to the foreign target. It states that the entity's name, any aliases, the source of the information, the date of the information, and who the foreign target is or has been in contact with should be recorded. The working aid argues that this helps prevent targeting, retargeting, inadvertent naming, or unauthorized metadata analysis, as targeting or naming a “protected” entity constitutes a privacy breach.

The practice of “protecting” Canadian information by classifying it as a separate category does provide some privacy protection. By flagging the person or identity, CSE arguably does prevent future privacy incidents if information from the person is captured in the future. However, this does mean that Canadian information is stored by CSE, even if it is not a direct target, as CSE holds the information that links it to a foreign target.

However, the working aid states that in exceptional circumstances, which it defines as threats to the security of Canada as defined in the CSIS Act or circumstances as described in OPS-1-10[6], the standard verification procedure can be bypassed (Communications Security Establishment 2014, 3). This would occur if there were a threat to life or an emergency and the standard verification procedure is not possible or takes too much time. This shows that standard privacy verification procedures can be circumvented in certain circumstances.

While there are many procedures regarding how to suppress CII and when to disclose it, there is also the question of who initially identifies CII through SIGINT and their role in CSE. CSE defines this type of SIGINT as “raw SIGINT.” Raw SIGINT is information directly collected

[6] The circumstances referenced are not present in OPS-1-10 or is redacted in the version released under ATIP used by this thesis.

through SIGINT activities without any evaluation or changes to protect privacy. The operations instruction document *CSOI-1-2: The Canadian SIGINT Production Chain and Access to SIGINT Data* displays who has access to raw SIGINT data. The document clearly states that access to raw SIGINT is limited:

> Access to raw SIGINT data must be limited due to the potential for exposure to information about Canadians, as well as the potential for compromising SIGINT methods, sources and capabilities (Communications Security Establishment 2013, 9).

The instruction document states that access to raw SIGINT data is limited to those who need it to fulfill their job requirements. Furthermore, privacy measures must be applied to raw SIGINT data to protect Canadian privacy (Communications Security Establishment 2013, 10). Based on the sensitivity of the information explained in the policy, Raw SIGINT information is likely only used by intelligence practitioners and not analysts. The information in raw SIGINT information is likely very compromising for the information it contains and the methods CSE uses to gather it. As stated in the policy, raw SIGINT information contains information on its methods and capabilities; such information is likely among the most guarded secrets of the organization.

Furthermore, according to the policy, personnel with access to raw SIGINT data must enact privacy measures regarding Canadian information. The policy states that, as part of their role in the SIGINT production chain, the personnel will: "Apply measures to protect the privacy of Canadians and ensure legal compliance in the conduct of their SIGINT activities…" (Communications Security Establishment 2013, 10). According to the policy, privacy measures are implemented as soon as CSE identifies Canadian information. However, as discussed above, CSE still keeps Canadian information.

CSE has many policies and procedures regarding its foreign intelligence mandate. Under its other mandates, CSE also collects and comes into contact with Canadian information, such as its cybersecurity mandate.

5.2.2 Cyberdefense/Cybersecurity

In its cybersecurity or cyber defence role, CSE collects Canadian information to defend against and investigate cyberattacks against the federal government. *OPS-1-6: Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports* sets out how CSE releases and

uses Canadian Identifying Information (CII) in reports created in its cyber defence role. The policy states that CII can be included in cyber defence reports if relevant or essential, including data containing recognized private communications, to identify, isolate, or prevent harm to a federal institution's computer system or networks (Communications Security Establishment 2010, 3). While the policy does not state what relevant or essential information is, it is likely information required to understand what the report is about. For example, in a report on a cyberattack on a provincial government, the name of the provincial government would be classified as CII, but naming the government would be essential to the report. A chart in the policy below details when suppressed or unsuppressed CII is to be in cyber defence reports.

1.5 When Must CII be Suppressed?

The following table sets out when CII must be suppressed from cyber defence reports. See paragraph 1.6 for information regarding naming exemptions.

If the report is to be disseminated to…	Then suppress and replace with a generic term…
the federal institution from which the information was obtained	N/A (No suppression required)
other federal institutions (including CSEC's Information Protection Centre)	**all CII,** except where • inclusion is relevant, or essential if it includes data containing a recognized private communication, for each recipient to use CSEC mitigation advice to protect their own networks, or • a naming exemption has been approved (see paragraph 1.6).
• Other CSEC areas (beyond the Cyber Defence Team) • Second Parties	**all CII**, except where a naming exemption has been approved (see paragraph 1.6).

Figure 2. CII Suppression in Cyber Defence Reports

The policy also states that exemptions are made for naming in cyber defence reports with prior approval of the Director General, Policy and Communications and the Deputy Chief, Information Technology Security. Thus, releasing Canadian information in Cyber Defense reports requires prior approval from the Director-General and CSE equivalent of the Assistant Deputy Minister level (Communications Security Establishment 2010, 4).

The procedure also states that the information must be suppressed when nationality is unknown and there are no apparent links to Canadian information. The analyst must use terms that state it may be Canadian information. The procedure gives examples such as "…'a possible Canadian IP address' or 'probable Canadian IP address' must be used" (Communications Security Establishment 2010, 4).

Like Canadian information collected under SIGINT operations, there is a process for releasing suppressed information from cyberdefence reports. While most of the process is similar, the rationale differs. Suppressed information from cyber defence reports can only be released "…if it is relevant or essential to protecting a federal institution's computer systems or networks" (Communications Security Establishment 2010, 7). While the policies regarding the collection and dissemination of Canadian information differ somewhat from their use with foreign intelligence, CSE is still required to protect the privacy of Canadians.

5.2.3 Assistance Mandate Policy

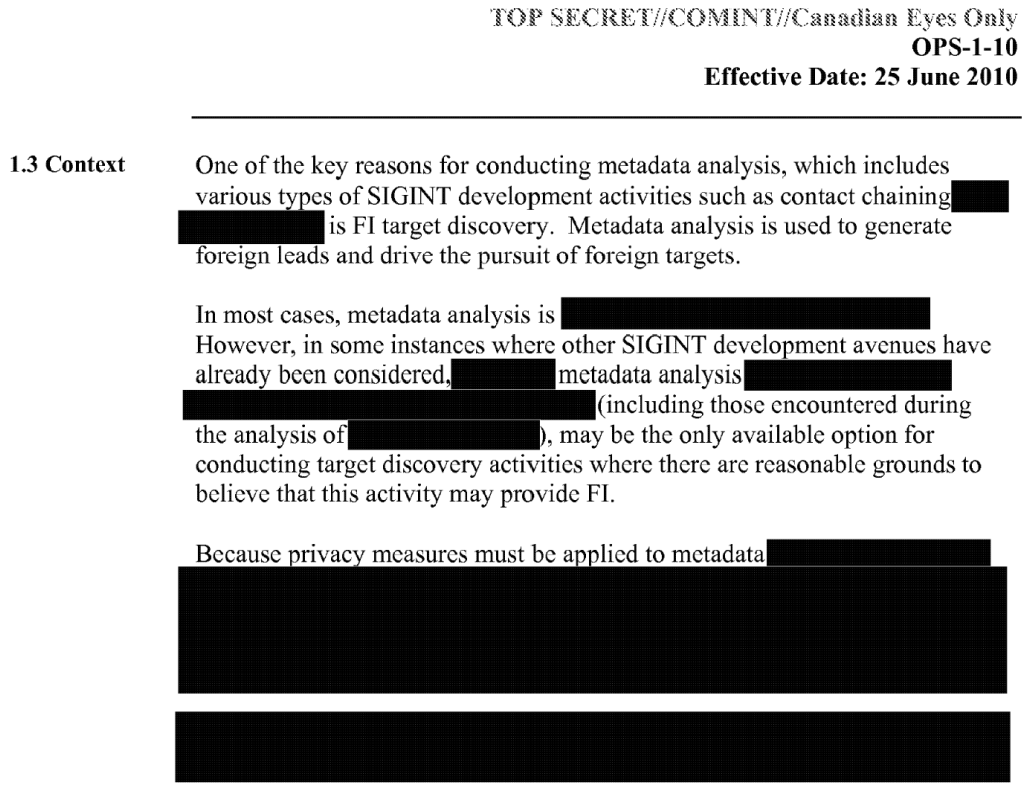
While most of the policies available for this thesis focus on the foreign intelligence mandate of CSE, some policies are available regarding the assistance mandate. The 2016 OPS-4: Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate gives insight into who CSE assists under this mandate and how assistance is carried out. The policy focuses on assistance to the RCMP and CSIS. To assist, CSE requires a written Request for Information from the agency. Also, the agency needs to state the authority to undertake the assistance requested and confirm that the information leading to the was lawfully obtained. CSE must assess the legal, policy and disclosure risks before approving the RFA (2016, 4). Under this policy, CSE must also review RFAs to ensure that if any RFA has an expiration date, any assistance must stop until a new RFA is submitted. If an RFA has no expiration date, CSE must review it annually. The policy also states that CSE cannot assist provincial, territorial, or municipal law enforcement agencies under its assistance mandate.

The operational policy notably lacks any information on privacy protections of Canadian information regarding its assistance activities; instead, it focuses on the lawfulness of the request. The policy states that CSE must be satisfied that the agency has the lawful authority to conduct the activity requests. As such, CSE must receive assurances that the requesting agency provides support to the RFA, which was obtained lawfully, to ensure that the requesting agency has the

legal authority to request the support (Communications Security Establishment 2016, 6). The policy states that citing the applicable legal authority (law), judicial authorization, or individual written consent constitutes a legal authority.

5.2.4 Metadata

There are also specific operational procedures for handling metadata.[7] While OPS-1-10: Operational Procedures for Metadata Analysis [REDACTED] provides insight, the privacy context is heavily redacted. The procedure states that metadata is used for contact chaining in order to find foreign targets. However, all additional methods are redacted. The figure below shows the available context.



TOP SECRET//COMINT//Canadian Eyes Only
OPS-1-10
Effective Date: 25 June 2010

1.3 Context

One of the key reasons for conducting metadata analysis, which includes various types of SIGINT development activities such as contact chaining [redacted] is FI target discovery. Metadata analysis is used to generate foreign leads and drive the pursuit of foreign targets.

In most cases, metadata analysis is [redacted] However, in some instances where other SIGINT development avenues have already been considered, [redacted] metadata analysis [redacted] (including those encountered during the analysis of [redacted]), may be the only available option for conducting target discovery activities where there are reasonable grounds to believe that this activity may provide FI.

Because privacy measures must be applied to metadata [redacted]

Figure 3. Context on Metadata Analysis

The procedure states that privacy measures must be applied, but further information is redacted, limiting understanding of how privacy impacts the metadata use procedure (Communications Security Establishment 2010, 4). Some other information is available, such as how CSE uses

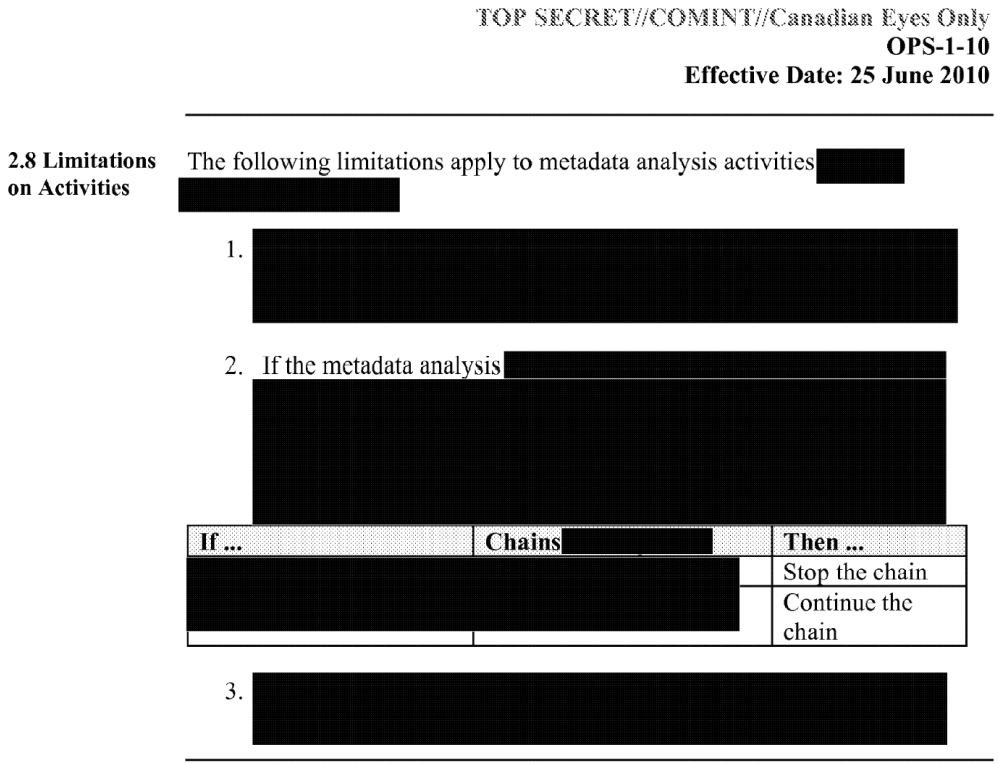
[7] Metadata is "data about data." It describes data but not the content of data. For example, metadata about a phone call would describe the two phone number, time, and length but not what was discussed.

metadata. The policy statement of the procedure asserts that metadata analysis, **when used for the foreign intelligence mandate** (emphasis added)**,** must comply with the laws of Canada and CSE Ministerial directives (Communications Security Establishment 2010, 4). Metadata analysis must never be conducted to obtain, produce or disseminate intelligence about a Canadian located anywhere or any person in Canada. Metadata analysis must also be subject to measures to protect the privacy of Canadians and be carried out only with the knowledge and express approval of CSE management (Communications Security Establishment 2010, 4). This policy only covers the use of metadata analysis for foreign intelligence. However, it is unknown if there are other policies for the use of metadata for CSE's other mandates. This policy only covers the use of metadata analysis for foreign intelligence. However, it is unknown if there are other policies for the use of metadata for CSE's other mandates.

If an analyst faces a target with an unknown nationality, the procedure gives two scenarios and instructions on how to proceed. However, the specifics of the scenarios are heavily redacted. The first states: "In cases where the nationality or location of the person [REDACTED] is difficult or not possible to determine [REDACTED] should be treated as relating to a foreigner located outside of Canada unless there are indications that it relates to a Canadian located anywhere or any person in Canada" (Communications Security Establishment 2010, 6). The second scenario states: " Conversely, the user [REDACTED] should be treated as Canadian unless there is strong evidence that the person is not a Canadian located anywhere or is not a person located in Canada" (Communications Security Establishment 2010, 6). These scenarios appear contradictory in nature, with one scenario stating that persons should be treated as foreigners while the other states they should be treated as Canadian. Additional context needed to understand the scenarios is likely part of the redacted text and may remove these scenarios' contradictory nature. However, from the limited information, CSE analysts seem to treat targets with unknown nationalities with some signs of being Canadian.

The approval process for metadata analysis is conducted at multiple levels. At the higher levels, the approval process goes through the analyst's supervisor, manager, or director, a redacted position, and finally is approved by CSE's "DGI" (Communications Security Establishment

2010, 9).[8] There is also a redacted section on the limitations of metadata activities, with almost no usable information to decipher. However, it does reference "contact chaining," noting that there are limitations to the contact chaining process. This section is presented in the figure below.


TOP SECRET//COMINT//Canadian Eyes Only
OPS-1-10
Effective Date: 25 June 2010

2.8 Limitations on Activities

The following limitations apply to metadata analysis activities [redacted]

1. [redacted]

2. If the metadata analysis [redacted]

If ...	Chains [redacted]	Then ...
[redacted]		Stop the chain
		Continue the chain

3. [redacted]

Figure 4. Limitations on Metadata Analysis

The same high levels of redactions are present in the section on the limitations of reporting the results of metadata analysis. The limitations of the first two sections of the report are entirely redacted, while other limitations do not provide much insight into how CSE distributes metadata. The only limitation of note states: "A client who has the lawful authority to [REDACTED] and produces appropriate rationale, may request and receive that information at the discretion of Operational Policy" (Communications Security Establishment 2010, 12). As with the limited information on how CSE distributes metadata, the policies regarding how CSE uses Canadian

[8] While there is no direct full title shown in non-redacted sections of the procedure, using general Government of Canada hierarchy nomenclature, DGI stands for Director-General Intelligence. Another document titled "DGI Familiarization Manual," provides a redacted organizational chart with the DGI title labeled Director-General Intelligence**Invalid source specified.**.

metadata contain heavy redactions. As such, any information regarding Canadian metadata, if located within this document, is unknown.

5.3 REPORTS

CSE is an organization that has several oversight and review bodies. Regarding privacy, before the passing of the Communications Security Establishment Act in 2019, the Office of the Commissioner of the Communications Security Establishment (OCSEC) was the oversight body of CSE. Currently, the National Security and Intelligence Review Agency (NSIRA) is the review body, and the Intelligence Commissioner (IC) acts as CSE's oversight body. Previously, the Commissioner of CSE was only a review body along with the Security Intelligence Review Committee. With the passing of Bill C-59 in 2019, the IC became an oversight agency for CSE and CSIS. This allowed for real-time oversight of CSE's activities rather than solely having review oversight.

Many of the reports used for my thesis research are from the former Office of the Commissioner of the Communications Security Establishment. Many of these reviews are relatively old, ranging from the 2000s to the 2010s. These reviews also provide a "historical" look at the conduct of CSE. However, many of the reviews that NSIRA conducts are released in a public format. These older reviews are used due to their availability. Many reviews from the Commissioner are public or released via past ATIP requests. As both NSIRA and the Intelligence Commissioner are new agencies, the reports available are limited, have not been released to the public, or have not been released under previous ATIP requests.

5.3.1 2011 SIGINT Targeting Review

In 2009, the OCSEC reviewed SIGINT targeting and selector[9] management activities. There is a caveat to using this report in this thesis research: the report is quite old at the time of writing, and the technology and policy have changed drastically since then. However, the report presents valuable research on historical issues and how CSE handled Canadian information at that time. The report goes into detail, abet heavily redacted, on how CSE uses, actions, and monitors SIGINT targeting and selectors. The report mentions concerns in a previous 2008 report on CSE activities. For example, policy and management aspects, including targeting and selector

[9] Selectors are identities used by a person or entity. The report states they include email address, IP addresses, telephone numbers etc. Additional examples of selectors are redacted in the report.

management, were areas of concern in the 2008 report, while other concerns were addressed (Office of the Communications Security Establishment Commissioner 2011, 3). Additionally, the report states that it found that CSE was following the law and had "sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) of any person in Canada" (Office of the Communications Security Establishment Commissioner 2011, 44). Additionally, the report states that it found that CSE was following the law and had "sufficient policies and processes to satisfy the legal requirement not to direct its SIGINT interception activities at a Canadian (anywhere) of any person in Canada" (Office of the Communications Security Establishment Commissioner 2011, 44).

Annex E provides a summary of privacy incidents reviewed by OCSEC. Almost all information is redacted, making even the timeframe unknown. However, given the size of the chart, there are likely few privacy incidents identified overall in the period the review covers. The annex shows the information CSE records when a privacy incident occurs. The annex indicates that CSE examines privacy incidents and finds possible areas of improvement. The figure below shows Annex E.

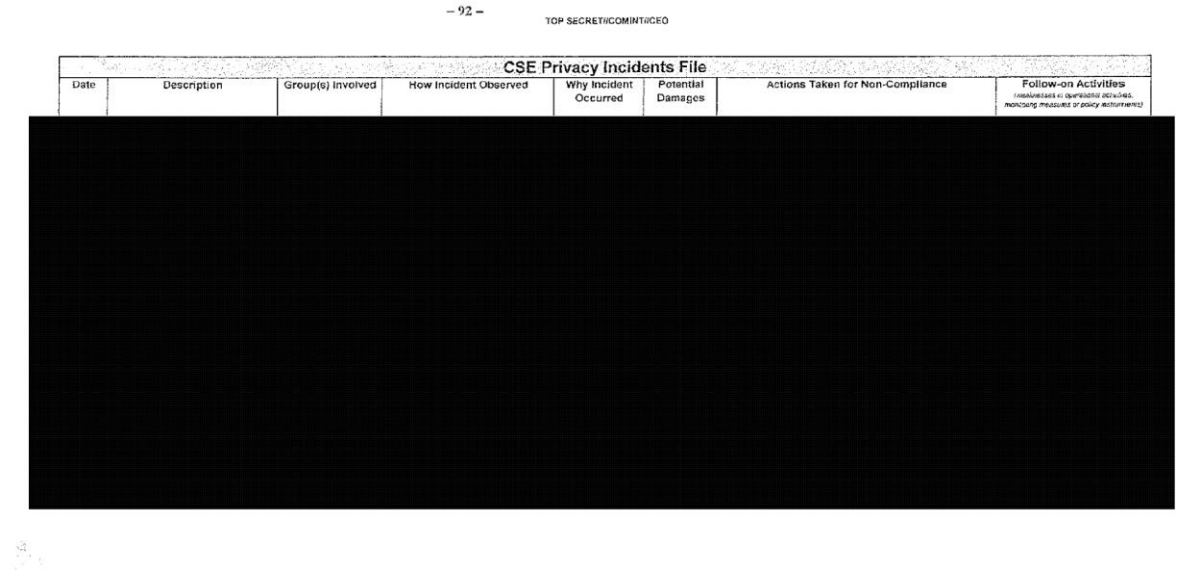


Figure 5. 2011 CSE Privacy Incidents

Overall, the review states that CSE followed policy and the law in its targeting process. However, the content and terms of this finding are not possible to analyze due to the lack of

disclosure. Future reports do show that privacy incidents have occurred. However, determining trends from public sources is difficult as not all provide the number of privacy incidents. For example, the 2016-2017 annual report does not provide the number of privacy incidents within CSE for that year, while the 2017-2018 annual report states that there were a total of 48 privacy incidents within that year (Office of the Communications Security Establishment Commissioner 2017, 26-29, Office of the Communications Security Establishment Commissioner 2018, 41-43).

5.3.2 2015 Assistance to CSIS Section 16 Review

In 2015, OCSEC reviewed CSE's assistance to CSIS under section 16 of the *CSIS Act*.[10] This review reveals how CSE assisted CSIS under section 16 and highlights issues with the process at that time. The report states that several areas of CSE support CSIS section 16 requests. As the report details, "Each area reviews the warrants, confirms the continued target association, analyzes traffic, prepares reports, refines requirements [REDACTED] …… and de-targets selectors on expiration of warrant or as directed by CSIS" (Office of the Communications Security Establishment Commissioner 2015, 7-8). Through some heavily redacted sections, how CSE provides technical assistance to CSIS is also reviewed when the report describes a specific request. "This request for technical assistance involves CSE providing processing [REDACTED] decryption for a specific [REDACTED] to make the traffic legible and to disclose the results of that processing or decryption to CSIS" (Office of the Communications Security Establishment Commissioner 2015, 9). In other words, this report states that CSE supports CSIS by decrypting traffic[11] and providing CSIS with unencrypted or legible results. This means that through CSE's assistance mandate, CSIS has the same technical capabilities as CSE. Any Canadian information provided by CSIS to CSE would be subject to CSIS's legal restrictions. The Commissioner explains this further in the report:

> CSIS may, in theory, use any collection method at its disposal to execute a warrant, subject to any limitations imposed by law in the performance of its duties. …CSE may provide assistance using any capability at its disposal, but the assistance provided is

[10] Section 16 of CSIS Act allows CSIS to gather intelligence on foreign state, but is restricted from targeting Canadians under Section 16.

[11] Traffic could be email, messages, etc.

> subject to any limitations imposed by law on CSIS (Office of the Communications Security Establishment Commissioner 2015, 14).

Furthermore, the report details how CSE handles Canadian information when assisting CSIS under Section 16. The report states it is CSE policy that all information about Canadians must be destroyed unless the information relates to a threat to the security of Canada under the *CSIS Act*, could be used in the prevention, investigation or prosecution of an alleged indictable offence, or relates foreign entities named in the request for assistance. As well, CSE cannot target Canadians under Section 16 warrants.

Overall, the review found that CSE complied with the law regarding its assistance to CSIS and followed policy. This finding does not mean that CSE did not have areas to improve. The review found that CSE and CSIS were basing their actions on a previous memorandum of understanding and not the most current one at the time of writing. While it is an arguably petty issue, it still highlights that CSE's collection and assistance activities have areas to improve.

5.3.3 Privacy Reports

In their role, the OCSEC and NISRA conduct reviews on CSE's activities to ensure they protect Canadians' privacy. These reviews can be annual reviews and ad-hoc reviews focused on specific practices.

In a 2008 report, OCSEC noted that its office was concerned that CSE treated information provided by CSIS the same as information collected under its foreign intelligence mandate. The OCSEC considered this a contravention of the 1990 memorandum of understanding between CSE and CSIS that was in effect at the time of the report (Office of the Communications Security Establishment Commissioner 2008, 10). The report notes that CSE is authorized to support CSIS in performing s.16 and s.12 activities under the *CSIS Act*. However, it identified several issues with corporate records practices. For example, OCSEC found no central database for CSIS Requests for Information (RFIs) (Office of the Communications Security Establishment Commissioner 2008, 9).[12] As such, CSE employees could not find information on why actions

[12] Requests for Information are official CSIS requests for intelligence from CSE.

were taken or if they were taken outside the scope of the original request. The lack of appropriate record-keeping produced difficulties in tracking and ensuring oversight of the RFI process.

The report also observed inconsistencies and omissions in the requests from CSIS for suppressed information. OCSEC found that in the requests from CSIS, the rationale for the request lacked proper information or was blank (Office of the Communications Security Establishment Commissioner 2008, 14). Further, in all instances, the section provided to indicate the law potentially or actually violated was left blank. The section requiring what actions may occur based on the information requests was also blank. The report states that this is a clear violation of CSE policy. The report states that CSE was within its mandate to assist CSIS. However, it found that some requests should have been enacted under the assistance mandate rather than CSE's foreign intelligence mandate (Office of the Communications Security Establishment Commissioner 2008, 15). This is quite concerning regarding both CSE's and CSIS's approach to the use of Canadian information gathered by CSE. It shows that both agencies disregarded policies meant to protect the privacy of Canadians. By leaving blank the section to indicate the law potentially or actually violated leads to the reasonable inference that CSIS was requesting information on a Canadian without proper justification or authority. It also demonstrates a lack of internal oversight by CSE when disseminating Canadian information to CSIS. However, future annual reports by the Commissioner show that CSE has addressed the issue of failing to provide justification for the request. The Commissioner's 2015-2016 annual report found that all requests for information by CSIS had proper justification (Office of the Communications Security Establishment Commissioner 2016, 18).

5.3.4 Annual Privacy Reviews

OCSEC and NSIRA conduct annual reviews of CSE privacy practices regarding Canadian information. These reports illustrate evolving issues and how new privacy issues can develop.

A 2014 review titled: *Annual Review of Disclosures by the Communications Security Establishment Canada of Canadian Identity Information from Foreign Signals Intelligence Reports to Government Canada Clients, Second Party Partners and Non-Five Recipients* provides insight into the privacy practices in CSE. It states that since 2008, CSE has disclosed CII lawfully, and policies and procedures have been put in place to protect the privacy of Canadians (Office of the Communications Security Establishment Commissioner 2014, 1-2).

There are several specific findings of note. The review found that CSE had no written policy regarding disclosing CII to non-Five Eyes recipients (Office of the Communications Security Establishment Commissioner 2014, 8).[13] However, this did not concern OCSEC as they are treated with the same scrutiny and need for rationalization as second-party requests. How this finding impacts Canadians' privacy is a question of risk, as well as raising concern as to whom the information is being sent. With second-party requests, the person to whom the information is being sent is known, as second parties are the members of the Five Eyes alliance. Third-party requests are unknown, as the state to which CSE sent Canadian information is unknown. This information is classified, making sending Canadian information to other intelligence agencies a transparency issue. Despite the legal protections of *Avoiding Complicity in Mistreatment by Foreign Entities Act* and OCSEC's lack of concern, there is an undeniable privacy risk in CSE sending Canadian personal information to other states, including the Five Eyes.

In contrast, a 2019 review found that the four instances of CII disclosure contradicted CSE policy. However, the report did not elaborate on how these reports contradicted CSE policy. The report followed up on a 2015-2016 report where "…CSE disclosed CII to [REDACTED] without obtaining sufficient information from [REDACTED] to substantiate its legal authority to collect CII nor an adequate operational justification demonstrating that [REDACTED] collection CII related directly to an operating program" (Office of the Communications Security Establishment Commissioner 2019, 2). The review found that the CII requests from the same entity now provided more information in its operational justification but failed to state the lawful authority needed to make the request (Office of the Communications Security Establishment Commissioner 2019, 3). The report also found that a redacted amount of CII requests from Government of Canada clients failed to state the lawful authority under which it was making the request (Office of the Communications Security Establishment Commissioner 2019, 6). In the review period, OCSEC also identified an instance of CII being disclosed to redacted Five Eyes or non-Five Eyes agency despite the official decision not being made by the proper approval authority (Office of the Communications Security Establishment Commissioner 2019, 7). In the review, OCSEC recommends that the CSE "… exercise enhanced diligence when disclosing CII outside of Canada" (Office of the Communications Security Establishment Commissioner 2019,

[13] Non-five eyes recipients are most likely foreign intelligence partners not in the Five Eyes community and not Government of Canada partners.

8). This report clearly shows that CSE has instances of improper disclosure of Canadian information. While the report states that it does not see the errors and improper disclosure as a systematic issue, future reports show that these issues are ongoing.

A 2020 review titled *Review of CSE's Self-Identified Privacy Incidents and Procedural Errors* found several issues in the privacy process at CSE. It found that:

> CSE has adopted a layered approach to increasing privacy protection measures. However, CSE is not using the PIF or any similar collated record of privacy incidents from re-occurring, or to identify any areas of weakness in existing policy and/or practice (2020, 3).

The report also found that each privacy incident was handled inconsistently. Specifically, it notes how the mitigation, documentation and reporting of privacy incidents were inconsistent and, at times, not assessed to determine the lawfulness or the privacy impacts on Canadians. Some incidents also focused on the deletion of the information rather than how the information was used. This is problematic as it focuses on removing improperly shared information rather than addressing whether there were reports or actions taken from the information. In other words, CSE focused on getting the bottle back after the genie was let out.

Furthermore, the report states that NSIRA does not expect CSE to have zero privacy or procedural errors, stating that the nature of CSE's activities makes privacy incidents unavoidable (2020, 5). While it is arguable that the nature of CSE's activities, SIGINT, makes it impossible for it never to collect Canadian information, it does mean that CSE has a great responsibility to protect Canadian's privacy. Out of all federal departments, CSE has the greatest capability to impact the privacy of Canadians. The privacy standards that CSE must maintain are rightfully high. However, there have been cases where CSE failed in this duty, as shown by several reports, including the one discussed below.

A 2021 unclassified and public version review of CSE's disclosure of CII by NSIRA provides more specific information on the CII disclosure process. The report states that it reviewed 2,351 disclosures made over five years. Of these disclosures, 28% did not meet the justification requirements for release (2021, 1). This means that one in four disclosures of Canadian information were improperly shared, representing a major breach of Canadian privacy. Assuming

that each disclosure was a different person, around 658 Canadians had their information improperly shared by CSE. The relatively high number of disclosures approved without proper justification arguably represents a pattern of CSE not following its procedures and failing in its legal duty to protect Canadian's privacy.

The report states that CII disclosures to Government of Canada clients did not have the same level of security nor documentation of the foreign requests. The report states that CSE did not have any analysis of the request, nor was there any documentation during the approval chain (2021, 4). The report also makes the point that CSE released additional personal information in addition to the requested information, and CSE noted this as a standard practice. The report recommended that CSE stop disclosing CII to Government of Canada clients outside the RCMP, CSIS, and the CBSA.

From these recommendations, it can be argued that NSIRA recommended that CSE stop sharing information with departments outside the Canadian national security community. Departments outside of the national security community likely lack the organizational understanding or culture of how to protect Canadian information received from CSE. This lack of understanding can be caused by the limited use of Canadian SIGINT information, resulting in a limited need to understand the sensitivity or legal restrictions CSE and other national security departments follow when handling such information. Thus, CSE sharing Canadian information with these departments leads to higher risks of privacy incidents and misuse of Canadian information. Furthermore, the report shows that CSE did not take internal dissemination of Canadian information within the federal government as seriously as it should have been. It is unknown if CSE now has policies and practices in place to scrutinize requests for information from other government departments. However, the fact remains that, from the information in the NSIRA report, CSE lacked care at the time of the report's dissemination of Canadian information. Sharing more personal information on Canadians than needed violates not only the privacy of the person involved but also increases the privacy impact as unneeded personal information is shared. Furthermore, there is also the impact of resulting actions taken based on improperly shared information. Depending on how the improperly shared information is used and how long the requesting agency has the information, the negative impacts on the person can be dire. Due to the scale of the possible impacts on a person due to improperly shared information means that

CSE and other Canadian intelligence agencies have a greater responsibility to protect the private Canadian information they hold and ensure they disseminate it with greater care.

The report included CSE's response to the review. It accepted the vast majority of the findings. However, CSE pushed back on what is best described as the "tone" of the review, stating:

> Without explaining the methodology used to support the findings, we are concerned that broad generalizations based on specific aspects of certain records within a single privacy measure may leave the reader with an incorrect impression about CSE's overall commitment to privacy protections for Canadian's (National Security and Intelligence Review Agency 2021, 11).

Furthermore, CSE claims it sent the records identified in the review to the Attorney General of Canada. CSE states that the Attorney General of Canada supports CSE in its activities and is in compliance with the *Privacy Act*. Lastly, CSE justifies its actions by stating:

> Top Secret-cleared and special intelligence-indoctrinated GC[14] clients received thousands of foreign intelligence reports via CSE's mandate under the *CSE Act*. These reports corresponded to Cabinet-approved intelligence priorities and were delivered to government clients who both had the authority to receive them and the 'need to know' their contents (National Security and Intelligence Review Agency 2021, 10).

The NSIRA review and CSE's response highlight how intelligence agencies and their review bodies can disagree regarding the operations of said intelligence agencies. From the CSE response to NISRA, CSE equates classification to protecting privacy. However, an employee with Top Secret clearance is not entitled to all top-secret information, and a department with a lawful request for a Canadian's information is not entitled to all information held by CSE about that person. The type of information shared by CSE is highly private and requires adequate protection by CSE. As stated by the CSE Commissioner in its 2019 report: "…the consequences of CII disclosure can be serious for the Canadian involved" (Office of the Communications Security Establishment Commissioner 2019, 8). CSE needs to take its legal obligation to protect

[14] Government of Canada

Canadian privacy seriously, as it has the greatest access to Canadian private information in the entire Government of Canada.

5.4 Conclusion

The authorities, policies, procedures, and review mechanisms regarding CSE's collection of Canadian information are complex, with differing legal and governmental instruments and policies dictating how Canadian information is collected, stored, accessed, and shared. However, several findings appear from these sources. From the reports and reviews by the various oversight and review agencies, there is a clear trend that CSE has issues with disclosing Canadian information. Each report found, to differing degrees, that CSE improperly shared Canadian information. The report of most concern is the 2021 NSIRA report, as it shows an increasing trend of improper disclosure when compared to the number of incidents in previous reviews. From the policy documents, it is clear that CSE has a robust policy framework regarding the retention and disclosure of Canadian information. Of note, CSE can routinely use Canadian information as long as it is "suppressed." This means that CSE uses Canadian information in SIGINT reports, which are shared outside of the department, so long as the Canadian information is anonymized. How these findings impact the privacy of Canadians will be further analyzed in the next chapter.

6. Analyses and Conclusion

Based on the findings of this thesis, it is clear that CSE collects Canadian information and, at times, targets Canadians under its assistance mandate. The nature of CSE being a SIGINT agency means it eventually encounters communications or information from a Canadian. Passive SIGINT, or a catch-all style of information collection, means Canadian information will be captured. Using the theory of privacy developed in Chapter 4, where privacy is the loss of control of personal information, CSE violates Canadians' privacy by the very nature of its work. There is a question on *why* CSE collects Canadian information and *why* CSE incidentally collects Canadian information. To answer this question, I will analyze CSE's activities using several previously outlined theories, such as Petit's theory of techno-securitization and Macnish's framework of just surveillance, as well as existing research. As outlined previously, *techno-securitization* and *everywhere surveillance* is global, it is a potentiality, and has complex geographies. I will also compare CSE's actions to Macnish's framework of just surveillance to determine, based on available information, if CSE's actions are just.

6.1 Does CSE respect Canadians' Privacy?

CSE does collect Canadian information. As previously stated, the nature of CSE's activities makes it inevitable that it will capture Canadian information. CSE and its oversight and review agencies know this fact and create policies to mitigate any privacy impacts to Canadians, as legally required. And yet, based on the findings of this thesis and compared to the definition of privacy developed in Chapter 4, CSE violates Canadian privacy by collecting Canadian information. What Canadian information CSE retains or deletes is heavily dependent on the discretion of CSE analysts, which denotes a lack of a standardized approach to Canadian privacy at CSE's initial collection of Canadian information. However, the more significant privacy impact is derived from it what does with the information. Legally, CSE is required to protect the privacy of Canadians' information it collects and, based on the findings of this thesis, it does so if it follows its own policies. Additionally, the majority of the privacy protections on Canadian information is based on *access* to information not retention.

6.1.1 Based on Primary Research

Legally and under its policy, CSE is not allowed to directly target Canadians unless assisting an outside department that is legally allowed to do so. Annual reviews by review and oversight agencies accessed for this thesis found that CSE did not break the law (Office of the Communications Security Establishment Commissioner 2018, 24, National Security and Intelligence Review Agency 2023, 15). Rather, CSE policies need to be developed to prevent privacy issues. Legally, CSE protects Canadians' privacy as determined by the *Communications Security Establishment Act* and the *Privacy Act*. It follows its responsibilities and requirements under the acts. To do this, CSE determines if the information provides foreign intelligence value. If so, any Canadian information is "suppressed," meaning CSE removes all identifying information. However, when read through the definition of privacy developed in Chapter 4, CSE clearly violates Canadian privacy through its collection of Canadian information.

As CSE is a foreign intelligence agency, Canadians are outside its core mandate. However, SIGINT's "collect it all" nature makes the non-collection of Canadian information impossible. Thus, CSE must collect Canadian information in some form. Due to this, CSE needs processes to delete Canadian information if it is collected. The policies reviewed by this thesis show that CSE has several policies and procedures to delete or surpass Canadian information as it is identified. However, it is unknown if CSE has tools or procedures to delete or suppress Canadian information at the point of collection. That said, there are risks to Canadians' privacy with CSE holding such information, such as the mishandling or unauthorized dissemination of Canadian information, which presents a considerable risk.

6.1.2 Natural Human Error

As with any organization that handles private information, privacy incidents at CSE can and do occur. All Canadian government agencies have policies in place to deal with privacy incidents. Privacy incidents can occur for various reasons, from human error, mishandling of information, or not following a policy. However, the nature of CSE's work means it has access to more private information than most government agencies. While the Canadian Revenue Agency can access a person's tax and financial information, CSE theoretically can easily access Canadian's private messages, online activities, metadata, and other electronic information. This level of access thus requires a higher standard of privacy protection that CSE must uphold when handling private information. And yet, although CSE must legally protect the privacy of the information it collects

from Canadians, the measures that must be taken are not included in the law. The only entity that determines if the privacy protection measures are adequate is the National Security and Intelligence Review Agency and its predecessor, the Communications Security Establishment Commissioner. There have been conflicts between the review agencies and CSE. OCSEC and NSIRA have faced difficulties obtaining information from CSE (National Security and Intelligence Review Agency 2023, 15). For example, in its 2022 annual report, NSIRA stated that it faced "…significant challenges in accessing CSE information on this review. These access challenges had a negative impact on the review" (National Security and Intelligence Review Agency 2023, 15). Such difficulties mean that CSE risks not having proper oversight and review. By withholding information from the oversight and review agencies, they cannot review said information to ensure CSE is following the law. As a result, when any information is withheld or not provided to oversight or review agencies, said agencies cannot be absolute in their confirmation that CSE is following the law.

6.1.3 From literature

While the policy and reports on CSE's activities show, based on known information, that CSE has followed the law and not actively violated the *Privacy Act* or its restrictions, secondary literature has shown examples in which CSE has possibly violated Canadians' privacy. Secondary research uses primary data that is not available to me, but it provides insight into the specific programs run by CSE. For example, as conveyed in CSE documents cited by Clement, CSE planned to use core[1] network hubs as part of its foreign intelligence mandate (2021, 138). Specifically, it planned to use EONBLUE sensors to collect traffic. However, Clement clearly does not claim that CSE is conducting mass domestic surveillance using Canadian carriers as "Single Source Operations (SSO)" (Clement, Limits to Secrecy 2021, 140). However, based on the information he analyzed, he strongly suspects that CSE has the capability to do so. Clement argues that CSE needs to be more transparent if it uses bulk collection programs in Canada. He also notes that what personal information is captured and how well it is protected is unknown.

From the policies and reviews of CSE's use and protection of Canadian information analyzed in this thesis, it cannot be proven without a doubt that CSE collects Canadian information in bulk

[1] CORE telecommunications hubs are major centers in which all telecommunications coming in and out of Canada are routed through.

nor conducts surveillance on a level comparable to the NSA's domestic surveillance programs. A review of the policies shows that CSE has stringent protections once it identifies Canadian communications. Any Canadian information it uses is suppressed, and it only shares unsuppressed Canadian information with partners who need to know and have the legal authority to do so. However, there remain questions about whether CSE conducts bulk collection, and these questions are left unanswered by the literature and CSE documents available. As Clement rightly notes, it is unknown how much Canadian information is captured by CSE bulk collection programs if they exist, which, as some literature shows, does occur.

Parsons and Molnar highlight the legal interpretation of CSE's bulk data collection programs of the past. They state that the CASCADE bulk collection program (which EONBLUE is a part of) was initially authorized as part of CSE's cyberdefense/cybersecurity mandate (Parsons and Molanr 2021, 242). However, CSE noted that it used CASCADE in all three of its mandates at the time (Parsons and Molanr 2021, 242). Outside of the debate on the legality of the CASCADE program, there is a relatively large privacy impact due to the program using deep packet inspection[2] to scan information passing through CASCADE sensors (Parsons and Molanr 2021, 241).

The literature and the Government of Canada disagree on whether CSE protects Canadians' privacy. Some scholars view CSE as threatening the privacy of Canadians. In contrast, others view CSE as conducting a delicate balance between what is authorized by the law and respecting the privacy of Canadians. Based on the information used in my research, I argue that while there are areas for improvement by CSE, the review and oversight agencies of CSE largely find CSE to comply with the law and adequately protect Canadian privacy.

Ogasawara's analysis of the evolving legal landscape of surveillance in Canada is an example of this disagreement. Ogasawara documents that Canada, starting after 9/11, allowed itself to conduct a higher level of surveillance, while also legalizing forms of surveillance that were previously deemed illegal. The secretive sharing of personal information, Ogasawara argues, goes against the recommendations of the Arar Commission (2022, 332). Ogasawara also argues that CSE's wiretapping under mandate A has no constraints (2022, 333). This claim is partly true,

[2] Deep packet inspection is a method of recording the content of data travelling through a network point.

as shown by the *CSE Act* and CSE's policies. For example, CSE can collect Canadian information incidentally when acting under mandate A and has to collect Canadian information in some form to determine if a target is Canadian. However, CSE cannot use mandate A to "wiretap" or target Canadians. Instead, it can incidentally collect Canadian information. Where Ogasawara is correct is that the legal exceptions for CSE that have expanded over time, such as its assistance mandate, legalize what can arguably be called illegal surveillance. For example, passed in 2014, Bill C-13 allowed the government access to internet subscriber information without a warrant (Ogasawara, Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence 2022, 334). This allowed the government to access information that previously needed a warrant freely. However, these exceptions often involve direct targeting, not mass surveillance. CSE's assistance to CSIS is one example. CSE has mandated restrictions against conducting surveillance on a scale considered mass surveillance.

6.2 Is CSE's Collection of Canadian Information Just?

Due to the redactions of information in documents reviewed in this thesis, it cannot be known fully how much Canadian information is collected and how it is used. The question remains as to whether CSE's collection of information is just. In this case, it can be justified in a normative ethical sense (Macnish 2014, 143). In order to determine if CSE's surveillance is just, I draw on Macnish's (2014) principles of just surveillance. Not all principles are used as not all principles apply to CSE. Additionally, I use available CSE's policies and procedures to determine if CSE's surveillance is just. This choice was made as information on the day-to-day operations of CSE is not available and documented policies provide a clear foundation to analyze compared to CSE actions, such as those documented in oversight reviews. Furthermore, CSE policies are temporally more consistent in comparison to other areas of reference.

The first principle is the principle of just cause. CSE exists for the state to protect itself in several ways. The cybersecurity and law enforcement assistance mandate are valid avenues for the state to protect itself. This mandate focuses on protecting the government's networks, thus being used in response to a hostile action. The law enforcement assistance mandate allows CSE to help Canadian law enforcement agencies enforce state laws. Cyber-attacks with the cybersecurity mandate and law enforcement with the assistance mandate are such avenues. It can be argued

that the collection of foreign intelligence under the foreign intelligence mandate is a way for the state to protect itself from outside threats. All three mandates can be considered a just cause for surveillance as they are ways for the state to protect itself.

The second principle is the principle of correct intention. It can be challenging to determine the intention of government departments. This is especially true for intelligence agencies, as their specific reasoning and goals are often classified. However, my review of CSE documents revealed some information on the intention of CSE's surveillance. CSE targets are based on both the Government of Canada's intelligence priorities and the requests of external agencies. However, the intention of individual targeting is not possible to know. However, high-level surveillance priorities are often based on cabinet-level priorities, which elected officials determine. Canadian information from the cybersecurity mandate would be collected concerning the protection of the Government of Canada networks. For example, if a person from Ontario attempted to access government networks illegally, CSE would collect that person's information to identify and stop them. Additionally, any action by CSE that would be illegal would need a Ministerial Authorization approved by the Intelligence Commissioner.

The collection of information under this mandate would have correct intentions as it would be used proportionally by the state to protect itself, as shown in the example above. How the information is used outside of the protection of government networks adds to the complexity of the principle. If the information is used outside of the original intention, it may depreciate the correct intention of the original collection. CSE's use of Canadian information outside its intended use would depreciate any "justness" under this principle.

The third principle is who is doing the surveillance and who is being surveilled. Macnish links this principle to just war. The state using surveillance for genuine national security would be just. However, should the state lose its moral authority to govern, it would become unjust (Macnish 2014, 148). CSE conducts surveillance and collects information on behalf of the state. As determined in the review of the documents, CSE conducts surveillance on foreign entities under its own mandate. It does not directly surveil Canadians under this mandate but does so under its assistance mandate. Under this mandate, the CSE does so on behalf of the requester, who has the lawful authority to do so according to policy. As CSE is an entity of the state, it conducts its role to protect the state's national security. Macnish notes that moral justification

comes from who is surveilling whom (citation). It is the scale and the target of the surveillance that determines the justness under this principle. An example of just surveillance under these three principles would be a person having a camera facing their driveway to deter theft. There is just cause: a homeowner can set up a camera on their property. There is also correct intention if it was only facing the driveway and is there to prevent theft or trespassing. It would also be just under the third principle as it would only surveil the homeowner's property and those within it. It does not violate the privacy of their neighbours or those on the street.

According to this principle, CSE can be considered just and unjust in its surveillance/information collection. Regarding foreign intelligence, CSE cannot target Canadians, but it can collect incidental information. Information collected and surveillance under this mandate can be argued to be just as the collection method is proportional to the amount and treatment of Canadian information.[3] This is proportional as Canadians are not directly targeted, and the incidental information kept must be protected and have foreign intelligence value. This results in limited justification for the collecting and keeping of Canadian information.

For its assistance mandate, where CSE directly targets Canadians, the justness of the surveillance rests in the justification of the law enforcement agency. This is due to CSE assisting law enforcement agencies within the legal restrictions placed on said agencies. As the specifics of such requests are unknown, it is difficult to determine the proportionality of the surveillance and who is being surveilled. However, using the information from some reviews of the assistance mandate, it is apparent that some assistance requests are arguably not just if they do not follow the policy. Under this principle, CSE granting support requests that do not follow CSE policies is unjust; thus, surveilling targets under unjust requests makes the surveillance unjust.

Macnish (2014) gives two principles for justifying the means of surveillance. The first is proportionality, discussed in Chapter 4, and the second is discrimination. With respect to surveillance, it is important to discriminate between legitimate and non-legitimate targets. According to Macnish, a legitimate target would be those threatening security or participating in criminal acts (Macnish 2014, 151). An illegitimate target would be those innocent of said acts. The principle of proportionality is that the level of surveillance is proportional to the context of

[3] As the focus of this thesis is on the collection of Canadian information, the argument and analysis of this principle is not including the justness of surveilling foreign entities.

the reason for the surveillance. It is almost impossible to determine how CSE deals with each target as case-by-case targeting requests are highly classified. With the principle of discrimination, Macnish argues that the only way to determine if a target is a valid target of surveillance is for the person to be surveilled in some form (2014, 151). CSE policy does address these two principles. CSE policy states that for an analyst to determine if a target is Canadian, the analyst must use the most unintrusive forms of surveillance. If the less intrusive forms of surveillance do not determine if a target is Canadian, the analyst can use more intrusive methods, with the most intrusive methods needing to be signed off by managers or directors.

Furthermore, how CSE targets and the level of intrusion on valid targets is unknown, as most tools and surveillance practices used by CSE are classified. As a result, it is unknown whether CSE conducts proportional surveillance on valid targets. This limits the ability of researchers, including me, to determine if CSE's surveillance is proportionate. However, when comparing CSE policy to the two above principles, CSE surveillance can be just and unjust. According to Macnish's principles, CSE's surveillance on possible targets, even to determine if the target is legitimate or not, would be unjust. As a result, the justness of CSE's surveillance would shift on a case-by-case basis. Furthermore, information on cases of CSE surveillance is not publicly available, thus making them impossible to analyze. However, since CSE surveillance is limited when attempting to determine if a target is Canadian, the unjustness of such surveillance would arguably be limited.

In summary, according to Macnish's principles of just surveillance, CSE is just to an extent and based on available information. When CSE does not follow the policies and guardrails that are in place, CSE's collection of Canadian information is unjust. The actions of CSE violate the privacy of Canadians based on the definition of privacy used in this thesis. However, violations of privacy do not necessarily make surveillance inherently unjust.

While CSE is arguably just, this argument is based on available information. The limits of available information means it is impossible to determine the justness of CSE's surveillance absolutely. Much of the information used to determine if CSE's surveillance is just is redacted. As a result, the determination that CSE conducts just surveillance is limited to what information is available and it is possible that redacted information could contradict my findings.

6.3 Theory of privacy and techno-securitization

In addition to analyzing whether CSE's surveillance is just, CSE's use and collection in the lens of privacy will be analyzed. First, as stated in Chapter 4, this thesis adopts the theoretical perspective that privacy is the right to control information; when a person loses control of their information without consent, their privacy is violated (Miller and Walsh 2016, 195; Sloan and Warner 2016, 370). Using this understanding, a person's privacy is violated when CSE collects Canadian information. However, anytime someone sends information using the internet, they are arguably losing control of their information as they rely on third parties to send the information. This is not to say that states and information technology companies have carte blanche to access someone's personal information or violate their privacy as soon as they access the internet. The idea of privacy in the current era is vastly more complex when digital information is included. In the information age, information is handled and controlled by a large number of parties when compared to the past. Several third parties may handle an email sent before it is received by the recipient. From the email service to the internet service provider of both the sender and the recipient, each step digital information takes to reach its destination is an area the state can surveille. Each step digital information takes can be an area in which a person's privacy can be impacted. The privacy impact of surveillance in the information age is not a question of whether the state has access but whether the state chooses to have access. Therefore, there is also the question of what the state does with the information and whether there are sufficient restrictions and procedures on sharing and use of information. How the state can use the vast digital network as a security and surveillance tool is best understood in Petit's theory of *techno-securitization*.

Petit's theory of *techno-securitization* provides insights for thinking through the impact of CSE's use of Canadian information. While Petit focuses on "*everywhere surveillance*" using the NSA, similarities exist as most technology is shared between the NSA and CSE (Communications Security Establishment 2014, 3). Using Petit's concept of *everywhere surveillance*, CSE's collection of Canadian information is just part of *everywhere surveillance*. *Everywhere surveillance* is global, and it is everywhere (Petit 2019, 49). Under *everywhere surveillance*, surveillance is global; it is a potentiality, and almost anywhere can become a surveillance site. Any piece of technology has the potential to become part of state surveillance. The power of the state to control aspects of the internet, such as core networking hubs, means the state, in turn, holds vast control of digital information. Privacy and the state in the information age is a

question of *whether* the state chooses to have access to information, thus choosing *if* it violates privacy. The increasing securitization of technology means that privacy depends on state restrictions, such as the legal restrictions on CSE.

As a result of *everywhere surveillance*, any Canadian information being transmitted globally will almost inevitably be captured as part of the securitization of technology. Everyone has the potential to be watched under *everywhere surveillance*, including Canadians by CSE (Petit 2019, 50). CSE policy and information documents show that under specific circumstances, CSE can directly target Canadians. As discussed by Petit, the current form of surveillance is global, as intelligence agencies use almost every form of technology to obtain information. Intelligence agencies like CSE and the NSA can access vast amounts of information remotely.

Petit highlights the tool TREASUREMAP, which allows an analyst to visualize the flow of the information of a target and with whom they communicate (Petit 2019, 45). Tools such as TREASUREMAP result from the need to process the vast amounts of information collected in the age of *everywhere surveillance. Techo-securitization* informs the privacy impact and level of access CSE has to Canadian information if it wishes to target Canadians due to the sophistication and access of CSE's surveillance capabilities. CSE arguably has access to almost all electronic information about a person and can target them via access to a person's phone to inspect information sent and funnelled through global information hubs. The *potential* information that CSE can access means that a Canadian targeted by CSE has all levels of their electronic information at risk. As many people are connected to devices and the internet in almost every aspect of their lives, the conditions for collection are vast and intimate. The sophistication of CSE's access to digital information means it has potential access to every facet of a person's life. It is through potential access made possible by *techno-securitization* that privacy risks arise. Under *techno-securitization,* the nature of CSE represents a privacy risk to Canadians. While CSE's nature is a privacy risk, ensuring that the surveillance is just ensures that the violation is limited and is not unwarranted.

6.4 Conclusion

CSE's access to vast amounts of information inevitably means that it collects Canadian information. The nature of CSE's role as a SIGINT agency, the shift to big data, and the vast volume of information collected by it and its Five Eyes partners mean it will access Canadian

information at some level. However, how it collects and uses this information is where the privacy risks to Canadians arise. Using the definition of privacy formulated in Chapter 4, CSE violates the privacy of Canadians; however, it is legally allowed to do so to an extent and must protect the private information of Canadians it does collect. The analysis of review agencies shows that CSE protects Canadians' privacy to an extent. However, the lack of information available to the public and, at times, review agencies means this conclusion is not definite. However, CSE's surveillance practices are arguably just under Macnish's principles of just surveillance as long as it follows its policies and regulations. CSE has the potential to be unjust as it can be just. When CSE does not follow its policies and regulations, privacy is impacted, as shown by improperly shared Canadian information with other government departments.

However, there are privacy issues even if CSE's surveillance and collection of Canadian information is lawful. It is unknown how much Canadian information is collected by CSE and what type of information that is. This type of information is highly classified and unknown to those outside of CSE. This makes it difficult to determine the exact level of private information CSE collects. It also makes it difficult to understand the scale of the collection. In past reports, NSIRA has published the number of requests CSE has received for Canadian information. However, these are only the requests and do not disclose the type of information being requested. CSE can collect Canadian information but discard it or suppress it for later use. Knowing the number of requests for Candain information does not show the collection scale from which the information originated. The fact that such information is highly classified means the public will likely never know the scale at which CSE collects information. This barrier shows the inherent limits of the ability of researchers (including me) to answer the question of whether CSE collects Canadian information and respects Canadians' privacy. CSE says that it protects Canadians' privacy. Where review agencies have determined that CSE has done so, they have also identified deficiencies and areas for improvement.

While there is a gap in scholarship on CSE, this thesis's research and analysis into how CSE collects, uses, and handles Canadian information bridges some of the gaps in current scholarship. CSE, by its very nature, is an opaque organization. The agency is not well studied compared to its counterparts; its impact on the privacy of Canadians, theoretical or realized, means it needs to be understood to both keep the agency accountable when Canadians' privacy is not protected.

There are areas where further research can shed light on CSE's impact on Canadians' privacy. Some of the policies used in this thesis are relatively old. Although many of the policies used, such as the OPS-1 policy suite, have been updated, the timeline for requesting these policies to be declassified under the *ATIPP Act* is long. Lengthy delays present a barrier to any academic study of CSE. Further research into the current policies of CSE regarding information could provide a much clearer picture of how CSE protects and respects Canadians currently, but this requires more effort on the part of CSE and the Canadian government, more generally, to provide timely processing of ATIP requests.

Appendix

Why Can States Spy on Each Other?

Why can CSE spy on foreign nationals and not Canadians? While writing this thesis, my supervisor asked this question, and it deserves exploration. This question relates to all foreign intelligence agencies and the idea of state espionage itself. Deeks gives three international law approaches to why states spy on each other. The first is the *Lotus Approach*, where nothing in international law prevents espionage. Deeks sums up this approach as:

> Several government officials and scholars believe that the Lotus
>
> approach provides the best way to think about spying in international law.
>
> For them, the idea is simply that nothing in international law forbids states
>
> from spying on each other; states, therefore, may spy on each other - and
>
> each other's nationals - without restriction. Spying is, therefore, unregulated in international law (2015, 301).

The second approach is where international law is permissive to espionage. This approach states that espionage is part of a state's role to defend itself and that the widespread use means states affirm the conduct (Deeks 2015, 302). The last approach to international law and espionage is that it is illegal. Part of this argument is that espionage for another state is almost always illegal in domestic laws. Several international treaties, such as the International Covenant on Civil and Political Rights and the Vienna Convention on Diplomatic Relations, arguably outlaw espionage.

Why states spy on each other, and the lack of restrictions on spying on each other is a topic of debate among scholars. However, Deeks's approach explains why CSE faces restrictions when gathering intelligence from Canadians and not foreign individuals. Spying on foreign individuals not in Canada is not covered under the *Charter of Rights and Freedoms,* nor do they have any legal protections.

Bibliography

Allen, Anita. 2008. "The Virtuous Spy: Privacy as an Ethical Limit." *The Monist* 3-22.

Austin, Lisa. 2015. "Lawful Illegality: What Snowden Has Taught Us about the Legal Infrastructure of the Surveillance State." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, by Michael Geist, 103-126. University of Ottawa Press.

Balzacq, Thierry, Sarah Léonard, and Jan Ruzicka. 2016. "'Securitization' revisited: theory and cases ." *International Relations* 494–531.

Bannister, Frank. 2005. "The panoptic state: Privacy, surveillance and the balance of risk." *Information Polity* 65–78.

British Columbia Civil Liberties Association. 2023. "Glossary of CSE Terms." *British Columbia Civil Liberties Association.* 03. https://bccla.org/wp-content/uploads/2023/03/Glossary-of-CSE-Terms.pdf.

Canadian Civil Liberties Association. 2015. *Understanding Bill C-51 in Canada: The Anti-Terrorism Act, 2015.* May 19. https://ccla.org/get-informed/talk-rights/understanding-bill-c-51-in-canada-the-anti-terrorism-act-2015/.

Clement, Andrew. 2021. "Limits to Secrecy." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, by David Lyon and David Woods, 126-146. Vancouver: UBC Press.

Clement, Andrew, Jillian Harkness, and George Raine. 2021. "Metadata - Both Shallow and Deep: The Fraught Key to Big Data Mass State Surveillance." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, by David Lyon and David Wood, 253-268. Vancouver: UBC Press.

Communications Security Establishment. 2019. *A Quick Guide to the CSE Act.*

2019. "Communications Security Establishment Act." *S.C. 2019, c. 13, S. 79.*

Communications Security Establishment Canada. 2009. "CSOI-5-8: Active Monitoring Procedures for [REDACTED]." *ATIPP Code: A-2017--01199.* Government of Canada.

—. 2012. "OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities." *ATIPP Code: 2017-00017--00215.*

—. 2012. "OPS-1-1: Operational Procedures for the Release of Suppressed Information from SIGINT Reports." *ATIPP Code: A-2017-00027--00188.*

—. 2012. "OPS-1-7: Operational Procedures for Naming in SIGINT Reports." *ATIPP Code: A-2017-00128.*

Communications Security Establishment. 2014. "CSE's International Partnerships: the 5-Eyes Relationships (Powerpoint)." *ATIP Code: A-2017-00017-03331.* Government of Canada, March.

—. 2013. "CSOI-1-2: The Canadian SIGINT Production Chain and Access to SIGINT Data." *ATIP Code: A-2017-0017--01454.*

Communications Security Establishment. 2013. *DGI Familiarization Manual.* Government of Canada.

—. 2010. "OPS-1-10: Operational Procedures for Metadata Analysis [REDACTED]." *ATIP Code: A-2017-00017--00044.*

—. 2010. "OPS-1-6: Operational Procedures for Naming and Releasing Identities in Cyber Defence Reports." *ATIP Code: A-2017-00017-00027.*

—. 2016. "OPS-4: Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate." *ATIP Code: A-2016-001-01--00003.*

—. 2014. "SIGINT Programs Instruction: Foreign Assessments and Protected Entities." *ATIP Code: A-2017-00017-01303.*

—. n.d. *Timeline.* Accessed July 27, 2024. https://www.cse-cst.gc.ca/en/culture-and-community/history/timeline.

Communications Security Establishment; Canada Revenue Agency. 2008. *Memorandum of Understanding between The Communications Security Establishment Canada and Canada Revenue Agency concerning Handling of SIGINT end-product reports.* Government of Canada.

Communications Security Establishment; Canadian Nuclear Safety Commission. 2009. *Memorandum of Understanding between The Communications Security Establishment Canada and The Canadian Nuclear Safety Commission concerning Handling of SIGINT end-product reports.* Government of Canada.

Connor, Brian, and Long Doan. 2019. "Government and Corporate Surveillance: Moral Discourse on Privacy in the Civil Sphere." *Information, Communication & Society* 52-68.

Deeks, Ashley. 2015. "An International Legal Framework for Surveillance." *Virginia Journal of International Law 55, no. 2* 291-368.

Department of Justice. n.d. *Section 8 – Search and seizure.* Accessed July 27, 2024. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html.

Geist, Michael. 2015. *Law, Privacy and Surveillance in Canada in the Post-Snowden Era.* Ottawa: University of Ottawa Press.

Gill, Peter, and Mark Phythian. 2018. *Intelligence in an Insecure World.* Cambridge: Polity Press.

Greenwald, Glenn. 2014. *No Place to Hide: Edward Snowden, The NSA, and the U.S. Surveillance State.* New York: Metropolitan Books.

Halperin, Sandra, and Oliver Heath. 2020. *Political Research: Methods and Practical Skills.* Oxford: Oxford University Press.

Leigh, Ian, and Njord Wegge. 2019. *Intelligence Oversight in the Twenty-First Century: Accountability in a Changing World.* London: Routledge.

Leman-Langlois, Stephane. 2021. "Big Data against Terrorism." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, by David Lyon and David Wood, 57-67. Vancouver: UBC Press.

Lyon, David, and David M Wood. 2021. *Big Data Surveillance and Security Intelligence: The Canadian Case.* Vancouver: UBC Press.

Lyon, David, and David Wood. 2021. "Introduction." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, 3-18. Vancouver: UBC Press.

Macnish, Kevin. 2014. " Just Surveillance: Towards a Normative Theory of Surveillance." *Surveillance & Society* 142-15.

Marx, Gary. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology.* Chicago: University of Chicago Press.

Matei, Florina, and Carolyn Halladay. 2019. *The Conduct of Intelligence in Democracies: Processes, Practices, Cultures.* Boulder: Lynne Rienner Publishers.

Miller, Seamas, and Patrick Walsh. 2016. "The NSA Leaks, Edward Snowden, and the Ethics and Accountability of Intelligence Collection." In *Ethics and the Future of Spying*, by Jai Galliott and Warren Reed, 193-204. New York: Routledge.

Mills, Jon. 2015. "The Future of Privacy in the Surveillance Age." In *After Snowden: Privacy, Secrecy, and Security in the Information Age*, by Ronald Goldfarb, 191-260. New York: St. Martin's Press.

Nath, Anjani. 2014. "Beyond the Public Eye: On FOIA Documents and the Visual Politics of Redaction." *Cultural Studies ↔ Critical Methodologies* 21-28.

National Security Agency. n.d. *UKUSA Agreement Release.* Accessed April 29, 2024. https://www.nsa.gov/Helpful-Links/NSA-FOIA/Declassification-Transparency-Initiatives/Historical-Releases/UKUSA/.

National Security and Intelligence Review Agency. 2023. *2022 Annual Report.* Annual Report, Government of Canada.

—. 2020. "Review of CSE's Self-Identified Privacy Incidents and Procedural Errors."

National Security and Intelligence Review Agency. 2022. *Review of the Communications Security Establishments (CSE) Ministerial Authorizations and Ministerial Orders Under the CSE Act.* Government Report, National Security and Intelligence Review Agency.

—. 2021. "Review of the Communications Security Establishment's Disclosures of Canadian Identifying Information." May.

O'Connor, Dennis. 2006. *A New Review Mechanism for the RCMP's National Security Activities.* Government Report, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.

Office of the Communications Security Establishment Commissioner. 2011. "A Review of CSEC SIGINT's Targeting and Selector Management Activities." *A-2017-00017--00995.*

Office of the Communications Security Establishment Commissioner. 2016. *Annual Report 2015-2016.* Annual Report, Government of Canada.

Office of the Communications Security Establishment Commissioner. 2017. *Annual Report 2016-2017.* Annual Report, Ottawa: Government of Canada.

Office of the Communications Security Establishment Commissioner. 2018. *Annual Report 2017-2018.* Annual Report, Government of Canada.

—. 2019. "Annual Review of Disclosures Canadian Identity Information for 2017-2018." *ATIP Code: AI-2022-00012.*

—. 2014. "Annual Review of Disclosures by the Communications Security Establishment Canada of Canadian Identity Information from Foreign Signals Intelligence Reports to Government of Canada Clients, Second Party Partners and Non-Five Eyes Recipients." *ATIP Code: A-2017-00017--01753.*

—. 2008. "Report to the CSE Commissioner on CSE Support to CSIS Phase I: CSE Mandate (a)." *ATIPP Code: A-2017-00017--00944.*

—. 2015. "Review of Communications Security Establishment Canada's Assistance to CSIS Under Part (c) of CSEC's Mandate and Section 16 of the CSIS Act." *ATIP Code: A-2016-00101-0017.*

Office of the Intelligence Commissioner. 2022. *Annual Report 2022.* Government of Canada.

—. 2023. "Intelligence Commissioner Decision and Reasons: In Relation to a Foreign Intelligence Authorization for [Redacted] Pursuant to Subsection 26(1) of the Communications Security Establishment Act and Section 13 of the Intelligence Commissioner Act." Government of Canada, April 21.

Ogasawara, Midori. 2021. "Collaborative Surveillance with Big Data Corporations." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, by David Lyon and David Wood, 21-42. Vancouver: UBC Press.

Ogasawara, Midori. 2022. "Legalizing Illegal Mass Surveillance: A Transnational Perspective on Canada's Legislative Response to the Expansion of Security Intelligence." *Canadian Journal of Law and Society* 317-318.

Parson, Christopher. 2015. "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance." *Media and Communication (Lisboa).*

Parsons, Christopher, and Adam Molnar. 2021. "Horizontal Accountability and Signals Intelligence." In *Big Data Surveillance*, by David Lyon and David Wood, 237-253. Vancouver: UBC Press.

Petit, Patrick. 2019. " 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization." *Science as Culture* 30-56.

Prince, Christopher. 2021. "On Denoting and Concealing in Surveillance Law." In *Big Data Surveillance and Security Intelligence: The Canadian Case*, by David Lyon and David Wood, 43-56. Vancouver: UBC Press.

1985. "Privacy Act." *R.S.C., 1985, c. P-21.*

Rimsa, Kostas. 2011. "Eavesdroppers." In *Inside Canadian Intelligence: exposing the new realities of espionage and international terrorism*, by Dwight Hamilton, 129-143. Toronto: Durdun Press.

Robinson, Bill. 2020. "The Communications Security Establishment (CSE)." In *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, by Stephanie Carvin, Thomas Juneau and Craig Forcese, 72-89. Toronto: University of Toronto Press.

Sharpe, Sybil. 2020. *National Security, Personal Privacy and the Law: Surveying Electronic Surveillance and Data Acquisition.* New York: Routledge.

Sloan, Robert, and Richard Warner. 2016. "The Self, the Stasi, and NSA: Privacy, Knowledge, and Complicity in the Surveillance State." *Minnesota Journal of Law, Science and* 347-408.

Stalla-Bourdillon, Sophie, Joshua Phillips, and Mark Ryan. 2014. "Privacy Versus Security… Are We Done Yet?" In *Privacy vs. Security*, by Sophie Stalla-Bourdillon, Joshua Phillips Phillips and Mark Ryan, 1-87. London: Springer.

The National Security and Intelligence Committee of Parliamentarians. 2022. *Annual Report 2021 (Revised version pursuant to subsection 21(5) of the NSICOP Act).* Annual Report, Government of Canada.

Warner, Margaret. 2013. *An exclusive club: The 5 countries that don't spy on each other.* October 25. https://www.pbs.org/newshour/world/an-exclusive-club-the-five-countries-that-dont-spy-on-each-other.

Watt, Eliza. 2021. *State Sponsored Cybersurveillence: The Right to Privacy of Communications and International Law.* Northampton: Edward Elgar Publishing.

West, Leah. 2020. In *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, by Stephanie Carvin, Thomas Juneau and Craig Forcese, 257-271. Toronto: University of Toronto Press.

Whitaker, Reg. 2015. "The Failure or Official Accountability and the Rise of Guerrilla Accountability." In *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, by Michael Geist, 205-224. University of Ottawa Press.

Williams, Stephanie. 2020. "The Powers of the CSE After C-59: Are Privacy Rights at Risk?" *National Journal of Constitutional Law* 131-151.

Wisnewski, Jeremy. 2016. "Wikileaks and Whistleblowing: Privacy and Consent in an Age of Digital Surveillance." In *Ethics and the Future of Spying*, by Jai Galliott and Warren Reed, 205-216. New York: Routledge.

X (Re). 2013. FC 1275 (Federal Court).