SAFE AND FREE:
NATIONAL SECURITY SURVEILLANCE AND THE RULE OF LAW ACROSS DEMOCRATIC STATES

The University of Texas at Austin
Strauss CENTER
for International Security and Law

CANADA'S NATIONAL SECURITY SURVEILLANCE REGIMES

Stephanie Carvin

ABOUT THE AUTHOR

Stephanie Carvin is an Associate Professor of International Relations at the Norman Paterson School of International Affairs.[1] Her research interests are in the area of national and international security. Currently, she is teaching in the areas of critical infrastructure protection, intelligence and public policy.

Stephanie holds a PhD from the London School of Economics and published her thesis as *Prisoners of America's Wars: From the Early Republic to Guantanamo* (Columbia/Hurst, 2010). Her most recent book is *Stand on Guard: Reassessing Threats to Canada's National Security* (University of Toronto Press, 2021) which was nominated for the 2021 Donner Prize for the best book in Canadian public policy. She is the co-author of *Intelligence and Policy Making: The Canadian Experience* (Stanford University Press 2021) with Thomas Juneau, and *Science, Law, Liberalism and the American Way of Warfare: The Quest for Humanity in Conflict* (Cambridge, 2015) co-authored with Michael J. Williams. From 2012-2015, she was an analyst with the Government of Canada focusing on national security issues. Her next project is a book on the Canadian far-right, co-authored with Queen's assistant professor, Amarnath Amarasingam.

ACKNOWLEDGEMENTS

This project was supported by funds from the Robert Strauss Endowment at the University of Texas at Austin and by a charitable gift from Microsoft. Each paper in the Safe and Free series reflects the views of its author. Editorial direction for the series was provided by Adam Klein, Director of the Robert Strauss Center for International Security and Law at the University of Texas at Austin. We are grateful to Strauss Center staff members Ali Prince and Brittany Horton, and to associate editors Zachary Badore, Seth Greenwald, and Taylor Helmcamp, for their help in shepherding the Safe and Free series to publication.

CONTENTS

NOVEMBER 2023

I. INTRODUCTION

Relative to most of its Five Eyes partners, Canada has a small and decentralized intelligence community. Nevertheless, Canada has substantial capacity for electronic surveillance both domestically and internationally. Many of the powers used by Canada's national security and intelligence agencies were clarified in the *2017 National Security Act*, which came into force in 2019. Today, Canada's national security surveillance and intelligence gathering activities are characterized by a powerful executive, minimal input from the legislature, and a complex set of rules that are increasingly showing their age. While there have been improvements in transparency, there remain serious gaps, which complicate the ability of legislators and civil society to scrutinize surveillance programs.

II. INSTITUTIONS[2]

Operational Entities

Canadian Security Intelligence Service (CSIS):
CSIS ("the Service") is Canada's domestic security intelligence service. It is mandated to collect information "within or outside Canada" related to threats to the security of Canada. Such threats are defined in s. 2 of the *Canadian Security Intelligence Service Act*[3] *(CSIS Act)* as espionage, foreign-influenced activities, terrorism,[4] and subversion. The Service is led by a Director who is responsible to the Minister of Public Safety.

Communications Security Establishment (CSE): The CSE is Canada's national cryptologic agency, making it similar to the US National Security Agency (NSA) and the UK Government Communications Headquarters (GCHQ). Under the *Communications Security Establishment Act (CSE Act)*, CSE has a four-part mandate:

- A: collecting foreign intelligence through the global information infrastructure
- B: protect the information and communications of the Government of Canada
- C: providing technical assistance to law enforcement, and;
- D: foreign cyber operations, including "active" (offensive) and defensive cyber operations.[5] CSE is headed by a Chief who is responsible to the Minister of National Defence.

Royal Canadian Mounted Police (RCMP): The RCMP is Canada's federal police force. It covers a wide range of criminal activity, including terrorism, espionage, and cyber-crime. While CSIS gathers *intelligence* on national security threats, the RCMP gathers *evidence* for national security prosecutions.

Department of National Defence/Canadian Armed Forces (DND/CAF): The Department of Defence and the Canadian Armed Forces are responsible for the defence of Canada at home and abroad. It has a large intelligence apparatus through its Canadian Forces Intelligence Command (CFINTCOM) to support its operations.[6] DND/CAF has the capability to collect both human and signals intelligence in support of its mandate to defend and protect Canada. It may also engage in counter-intelligence activities.

Although it is one of the country's largest intelligence agencies by size, all of DND/CAF's intelligence activities must have a "clear nexus" with its operational activities and mandate. In other words, it is not a truly autonomous foreign intelligence agency.[7] The CAF can also support the intelligence collection activities of other government departments and agencies, such as CSIS or the RCMP, at the formal request of the Minister of Public Safety, while operating under the authorities of those agencies.[8]

Although it is one of the country's largest intelligence agencies by size, all of DND/CAF's intelligence activities must have a "clear nexus" with its operational activities and mandate. In other words, it is not a truly autonomous foreign intelligence agency.

Authorizing Entities

Ministers: In Westminster systems, cabinet ministers, who are almost always also members of parliament, are responsible for authorizing strategic and operational collection priorities. In the context of intelligence and national security, ministers may be asked to approve certain operations and missions that are high-risk and dangerous, and in this way provide a degree of oversight – albeit one that does not often see the light of day. Canadian ministers typically have fewer staff than their American counterparts. In this sense, when it comes to evaluating the advice of the civil service, the outcome will depend on the quality of the minister and the staff they hire.

In addition, the influence of "the Centre" (Treasury Board, Privy Council Office, and Finance Department, and especially the Prime Minister's Office) may mean the minister will find their influence curtailed by the centre and their Cabinet colleagues. In this way, despite being in charge of a file, they may struggle to find an alternative to what the public service presents or find their plans on hold for other government priorities.

Ministers also direct and authorize the collection activities of some agencies, even agencies that are not directly in the minister's portfolio. For example, (as will be discussed below) at the "personal request in writing" of the Ministers of Foreign Affairs, Defence, and Public Safety, the Service may collect information within Canada as it relates to foreign states, a group of foreign states, and/or non-Canadian persons/permanent residents.[9] In addition, the Ministers of Foreign Affairs and Defence play an important role in the authorization of certain foreign cyber operations. The Minister of Public Safety also has a role in approving certain domestic operations where a warrant is required.[10]

Intelligence Commissioner: The Intelligence Commissioner (required to be a retired judge of a superior court) serves a quasi-judicial role by overseeing CSE activities to ensure that they comply with Acts of Parliament and respect the reasonable expectations of privacy of Canadians and anyone in Canada. This includes reviewing the reasonableness of the Minister of National Defence's authorizations as well as the classes of "datasets" – electronic information depositories – that the Minister of Public Safety authorizes CSIS to receive. This responds to the need for independent judicial or quasi-judicial oversight of intrusive intelligence activities required by section 8 (s. 8) of the *Canadian Charter of Rights and Freedoms* (the right to be free from unreasonable search and seizure, discussed further below).

Courts: Courts straddle the divide between control (issuing or denying warrants), oversight, and scrutiny (in their regular role as courts of judicial review). Judges play an important role in authorizing surveillance and the use of intrusive investigative means. Although their collection activities may be similar, the warrant regimes for CSIS and police/RCMP are very different. Requesting authorities for police investigations typically must demonstrate that an individual or entity is engaged in a crime. Police warrants are issued by judges at the provincial level. By contrast, only the Federal Court issues warrants for intrusive search and seizure activities by the Service.[11]

Finally, each department or agency that engages in collection will have its own policies and procedures which internally govern these activities. For example, senior management (often Directors General or "DGs") will be required to sign off on plans for collection and investigations.

Oversight Entities

In Canada, the terms "oversight" and "review" are often used interchangeably but have defined and unique meanings:

> Review refers to the ability of independent bodies retrospectively to evaluate security activities. A reviewer does not have operational responsibility for what is being reviewed… Oversight refers to a command and control process – the power to issue directions, influencing conduct before it occurs. Review bodies do not have the power to oversee anti-terrorism activities, thought they can make findings about failings and can make recommendations on improvements.[12]

Therefore, most "oversight" institutions in Canada are review bodies, and oversight functions (almost entirely, but not exclusively) rest with ministers (usually of National Defence, Foreign Affairs or Public Safety) and the Intelligence Commissioner. Additionally, as discussed below, the federal courts play an oversight role through approving CSIS warrants.

National Security and Intelligence Committee of Parliamentarians (NSICOP): NSICOP is the first permanent review body made up of democratically elected representatives in Canada. The Committee, (governed under its own Act[13]) is a committee of Parliamentarians (though not a Parliamentary committee).[14] It is part of the executive branch, although it is comprised of members of the legislative branch, and their reports are ultimately released through the Prime Minister's Office. NSICOP has the mandate to review the legislative, regulatory, policy, administrative, and financial frameworks for national security and intelligence. The Committee may also review the activity of any government department relating to national security or intelligence (unless it is part of an ongoing operation or an investigation whose disclosure is deemed injurious to national security by the relevant minister) or any matter relating to national security and intelligence referred to the Committee. For example, it has done in-depth reviews

of defence intelligence activities in Canada,[15] produced special reports on controversies (such as the role of intelligence agencies in Prime Minister Justin Trudeau's visit to India in 2018),[16] as well as an annual report.[17] A director and secretariat support the work of the Members of Parliament composing the committee. At present in Canada there is pressure to remake NSICOP into a parliamentary committee (a legislative body), modeled on the UK Intelligence and Security Committee.[18]

National Security and Intelligence Review Agency (NSIRA): By statute, NSIRA is tasked with assessing compliance of the national security and intelligence community with the laws of Canada.[19] Unlike its predecessors, NSIRA has the power to review any activities performed by CSIS, the CSE, and any other national security or intelligence-related activity carried out by federal departments and agencies. NSIRA is comprised of up to seven part-time members and is supported by a secretariat. NSIRA differs from NSICOP in that the former is concerned with compliance, the latter with efficacy–although this is by practice and not defined in any statute. Like NSICOP, NSIRA issues an annual report,[20] agency-specific reviews,[21] and investigations into special issues, such as the treatment of Canadian identifying information by the CSE.[22]

Parliament: The concept of "scrutiny" is relevant to this discussion, although it plays a less important role in the Canadian context relative to Canada's Five Eyes partners. In Westminster systems, scrutiny ensures political accountability: members of a law-making body ask questions or scrutinize the government (whose ministers sit as members of those bodies), often but not exclusively in the legislative chamber. In Canada, ministers are accountable to Parliament for the performances of the departments and agencies under their control.

Parliamentarians can scrutinize government department or agency performance through committees in the House of Commons and the Senate. Ministers and senior bureaucrats can be called to answer questions and provide details about an operation or issue.[23] However, as most Canadian members of parliament and senators are not provided with a security clearance, they cannot discuss or have access to classified information. As such, the ability for committees to engage in robust scrutiny is limited. However, scrutiny remains important in that may bring important issues to the public's attention.

Departments and agencies: Each department and agency has its own policies and procedures and review policies. Some, like CSIS, have an Internal Audit department which provides advice on risk management and performs evaluations of operations and programs.[24]

Auditor General and Privacy Commissioner: The Auditor General and the Privacy Commissioner are officers or "agents" of Parliament, charged by their governing statutes to report directly to Parliament on matters within their remit. They conduct periodic independent audits of federal government operations, including government departments.[25] Both positions have limited capacity, however, and do not always have the expertise and resourcing to delve into the complicated world of intelligence operations and national security.[26]

III. OPERATIONAL CAPABILITIES AND PRIORITIES

Canada is a technologically advanced country with sophisticated capabilities to engage in domestic surveillance at home and assist in Five Eyes operations abroad. Legislative reforms in 2019 authorized CSE to undertake active cyber operations, for such purposes as disrupting communications between violent extremists or protecting Canada's democratic institutions.[27] In 2020, the Harvard Belfer Center ranked Canada eighth in the world in terms of its cyber capabilities, placing it third among Five Eyes countries after the United States and the United Kingdom.[28] The CSE produces approximately 10,000 end product reports (EPRs) each year, a large proportion of which are shared with Five Eyes countries.[29]

The main limitations on Canada's surveillance activities reflect its small size relative to other countries, as well as the limited mandates of some organizations. Most notably, CSIS is highly restricted in the security intelligence it can collect outside of Canada. As such, Canada is dependent on its allies, especially its Five Eyes partners, for much of its foreign HUMINT intelligence collection.

Intelligence Priorities Process: Canada's intelligence priorities are set every two years by a Cabinet committee. The committee's composition has changed over time per the preferences of the Prime Minister.[30]

IV. PROCESS FOR APPROVING SURVEILLANCE

While CSIS is responsible for gathering *intelligence*, the RCMP gathers *evidence* for criminal prosecutions through a separate but parallel process in national security investigations. This division of labour means that while the surveillance powers each agency possesses are similar, the authorization regimes to use them are very different.

Collection Against Domestic Targets

RCMP: The RCMP's national security criminal investigations are conducted by the National Security Enforcement Sections (NSES) within RCMP divisions or by Integrated National Security Enforcement Teams (INSETs) located in Ottawa, Montreal, Toronto, Edmonton/Calgary, and Vancouver.[31]

Interception

Police powers to engage in intrusive surveillance range from physical surveillance, the use of cameras and recording equipment, and the interception of communications. Recently, it was revealed that in some cases the RCMP uses malware or "spyware" to hack phones in order to obtain text messages, email, photos, videos, audio files, calendar entries, and financial records, as well as to gather audio recordings and take pictures.[32]

The key framework for the authorization of interception powers is Part VI of the Criminal Code, which applies to any investigation where a "private communication" will be intercepted.[33] The Criminal Code defines a "private communication" as any oral communication or "telecommunication" (including wire, radio, optical, and cable communications) "made by an originator who is in Canada" or intended "to be received by a person who is in Canada" and "made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person" other than the intended recipient.[34]

Importantly, this definition is interpreted broadly to include any information deriving from the communication that would convoy its substance or meaning.[35] In addition, how the police may access the private communication depends on the transitory state of the information – whether it is being intercepted or seized. Where a communication is being intercepted in transit, the Part VI warrant is required. However, where an archived private communication is being stored on a device, a different seizure regime, production orders," applies, as will be discussed below.

Like standard warrants, Part VI authorizations for interception are approved by judges at the provincial level. The authorities requesting must show reasonable and probable grounds for authorization. However, given the intrusive nature of such collection activities, there are additional constraints. The judge must be satisfied that the granting of the authorization would be in the best interests of justice and that other investigative procedures have been tried and failed, are unlikely to succeed, or that the matter is so urgent it would be impractical to investigate using only other procedures.

Applications for Part VI warrants require an affidavit where full disclosure must be made. This includes the proposed manner of interception, all places reasonably expected to be encountered over which the target may not exercise exclusive control, terms and conditions to ensure privacy of uninvolved persons, and whether surreptitious entry is being proposed to install, maintain, or remove electronic surveillance equipment.[36] These applications are made in a closed court on an *ex parte* basis, with only the government side represented.

Importantly, there are special rules for the surveillance of criminal organizations and terrorism investigations. The "last resort" obligation is not required in these cases.[37] Additionally, while authorization for electronic surveillance may not exceed sixty days, interception warrants targeting criminal organizations or terrorism investigations may last up to one year. Moreover, unlike other cases, obtaining an extension for a warrant is not dependent on the persistence of an ongoing investigation.[38]

Special care must be taken where interceptions may involve "communications of a sensitive nature." This includes possible infringements of the privileges or immunities of members of Parliament, Senators, or other legislators. In these cases, prior legal advice must be secured from the Attorney General of Canada, who will advise the Minister of Public Safety and Emergency Preparedness. In addition, particular attention must be paid to potential violations of solicitor-client privilege.[39]

Finally, Part VI warrants differ from other warrants in that authorities must ultimately notify the target of the surveillance.[40] Within 90 days after the surveillance ends, the authorities must notify in writing the person who was the object of the interception. However, this may be delayed up to three years by a judge upon application by the Minister of Public Safety. The judge must be satisfied that the investigation of the offence to which the authorization relates is continuing. However, with terrorism cases the investigating authorities are not required to demonstrate the persistence of an ongoing investigation for an extension.

Lawful Seizures from Third Parties

A separate but related regime relates to the seizure of electronic information through "production orders," a form of judicial authorization compelling the holder of specified information (such as a telecommunications provider) to disclose that information to police. They are required when police need information from a third party and where a potential infringement on a person's reasonable expectation of privacy may arise. This includes basic personal information, like subscriber data associated with an ISP address.[41]

Production orders apply to records that already exist (data-at-rest) rather than those which may exist in the future or are in the process of being sent (data-in-motion). This can sometimes create challenges determining which legal regime is applicable to access the same kind of information. For example, where police seek to collect text messages or emails that are not in existence of the time of the order, or still capable of delivery ("in motion"), the intercept regime applies. However, where archived text messages or emails are stored by a service provider (data is "at rest"), production orders may be used. Importantly, law enforcement may not use production orders to side-step the more onerous Part VI regime.[42]

There are several kinds of production orders, including orders for paper and electronic documents, orders for financial information, and orders for transmission, tracking, and trace information. For the purpose of this paper, the latter is the most significant. Transmission refers to information about telecommunications including the type, direction, date, time, duration, size, origin, destination, or termination of the communication but does not include the content of communications.[43] Tracking data relates to the location of a transaction, individual, or thing. Trace information is data for the purpose of identifying a device or person involved in the transmission of a communication that will assist in the investigation of a suspected offence.[44]

> ***Applications for general production orders are made on an ex parte basis to a judge who must be satisfied that there are reasonable grounds to believe an offence has been or will be committed and that the document or data in the person's possession or control will afford evidence respecting the commission of the offence.***

Applications for general production orders are made on an *ex parte* basis to a judge who must be satisfied that there are reasonable grounds to believe an offence has been or will be committed and that the document or data in the person's possession or control will afford evidence respecting the commission of the offence.[45]

However, the threshold to obtain a production order for "transmission, tracking and trace" information is lower. Only reasonable grounds to suspect are necessary.[46] So far, the Supreme Court of Canada has allowed this lower threshold as these searches are considered "minimally intrusive, narrowly targeted, and highly accurate."[47] Yet, some scholars have questioned if this standard can still apply to an era of increasing data analytics and large quantities of metadata.[48]

Finally, when it comes to electronic devices, it is not enough for police to obtain a search warrant at a home or office to access them. Instead, a separate warrant is needed to search electronic devices specific to a location.[49] Once that warrant is granted, police may search the data contained within the computer, but also search information available to the computer system, including cloud-based applications and other online or networked

accounts accessible from the device.[50]

CSIS: Within Canada, the most important collection authority the Service has is its ability to "target" an individual, person, organization, or event suspected of constituting a threat to the security of Canada.[51] Targeting activities, which include methods of varying intrusiveness, including electronic surveillance and physical searches, are governed by the rules and procedures set out in the CSIS Act, ministerial directives, Service policy, and other related procedures.[52] In carrying out collection the Service must follow the rule of law, proportionality of means, use the least-intrusive techniques first (with the exception of emergencies), and the level of authority required must "be commensurate with their intrusiveness and risks associated with using them."[53] In addition, if any investigation involves "sensitive sectors," such as educational and religious institutions, extra layers of approval will be required.[54]

CSIS authorities to collect information may be divided into two categories. First, there are those short of a warrant, where techniques used do not violate the reasonable expectation of privacy guaranteed by Section 8 of the Charter. This is usually for cases where investigators have reason to suspect an individual may be engaged in threat-related activity. Here, collection is governed within the Service and typically require approval by a senior official holding the rank of Director General. The authorities are divided into different investigative levels: Level 1 allows for basic information gathering, while Level 2, which allows for more intrusive means, including physical surveillance. According to CSIS documents released under the Access to Information and Privacy (ATIP) process, several factors are considered when selecting the appropriate targeting level, including the nature, imminence, and significance of the threat, the collection techniques allowed, and the availability of resources to conduct the investigation.[55]

Second, once the Service moves from "suspecting" that an individual or individuals might be engaged in threat-related activities to the point where it "believes" that they are doing so, it can seek to use more intrusive means. This can include electronic surveillance for which CSIS can apply to the Federal Court for a warrant under s. 21 of the *CSIS Act*.

The process to obtain a warrant can be lengthy; applications often run more than 50 pages, and every line must be supported ("facted," in Service jargon) with evidence. DOJ lawyers vet the applications rigorously, and they are subject to several layers of management approval. In addition, Service personnel are often required to testify to the information in the warrant and answer any questions federal judges[56] may ask. While this is typically a lengthy process, the system can move quickly if needed, particularly in the wake of a serious incident.[57]

The reason for this demanding process is clear: First, unlike police warrants, the information collected in surveillance operations is not intended to ever be used in court. Second, unlike Part VI warrants, there is no notification requirement that the surveillance took place.

Unfortunately, in recent years, designated judges have found on several occasions that the Service has failed in its "duty of candour." In other words, the court found that CSIS had failed in its legal obligation to present all relevant information that the court needed to engage in proper oversight. A review of this issue by NSIRA in June 2022 found deep-seated problems with the way the Service and its counsel, Department of Justice (DOJ) lawyers, organize themselves.[58] While DOJ lawyers often failed to provide timely and accessible advice, particularly in urgent situations, CSIS has failed to professionalize the warrant application process sustainably and fully as a specialized trade that requires training, experience, and investment.[59]

Datasets: The regime which regulates the way CSIS handles datasets is one of the most complex aspects of the Act. To address concerns about the changing nature of information, how it is generated, collected, searched, and stored, and how all of this relates to national security investigations, the 2017 *National Security Act* creat-

ed a "dataset" regime. It provides legal authority for the receipt and retention of information that is not definitively threat-related but may be of some value overall. It does so by setting out how datasets may be retained and the subsequent searching of that data to make it s.8 compliant (although this has yet to be tested in court.)

Under s. 2 of the *CSIS Act*, a "dataset" is a "collection of information stored as an electronic record and characterized by a common subject matter."[60] The dataset regime sets out three categories: publicly available information, Canadian (involving citizens and persons in Canada) and foreign (non-Canadians outside of Canada). Before retaining the dataset, the Service must determine that it is related to their performance and functions under its *Act*. In addition, with Canadian datasets, the Service must determine that it falls under a list of pre-approved classes of data as determined by the Minister of Public Safety and approved by the Intelligence Commissioner as "reasonable."[61]

Unless there is a life-threatening emergency present, the Service must wait 90 days before using the dataset. The 90 days provides the Service a window to determine the relevance of the dataset to an ongoing investigation and to prepare an application for its use. It may also clean up the data available, such as translating, decrypting, or deleting erroneous or poor-quality information. Information relating to physical or mental health, or any information related to solicitor-client privilege must be deleted. In any foreign dataset, all information involving a Canadian must be destroyed or treated or submitted as a Canadian dataset.[62]

> ***To retain a Canadian dataset for longer than 90 days, the Service must obtain an authorization from a Federal Court judge which, if granted, may last up to two years (renewable). To retain a foreign dataset, the Service must obtain authorization from the minster and approval of the reasonableness by the Intelligence Commissioner.***

To retain a Canadian dataset for longer than 90 days, the Service must obtain an authorization from a Federal Court judge which, if granted, may last up to two years (renewable). To retain a foreign dataset, the Service must obtain authorization from the minster and approval of the reasonableness by the Intelligence Commissioner. The foreign dataset approval lasts for five years and may be renewed.

Queries of the dataset must be done on a strictly necessary basis, and results must be deemed strictly necessary to be retained.[63] The legislation envisions two kinds of queries. First, specific searches related to a person or entity within the dataset. Second, "exploitation" – computational analysis to obtain intelligence that would not otherwise be apparent.

One Vision: Unlike the Service, the purpose of RCMP national security investigations is for the collection of evidence to be used in court. However, while this process is ongoing, it is often the case that CSIS will continue its intelligence gathering operations, albeit in a way that does not interfere with the RCMP's investigation. As Canada's laws guarantee that the Crown will disclose to the accused all relevant information used in its criminal investigation, the Service will be extremely cautious in what intelligence it provides to the RCMP out of concern that this may end up in court. When it does so, CSIS will provide a "disclosure letter" containing information designed to be used as a lead – a formalized version of a "tipoff."

The Service may also provide an "advisory letter" to the RCMP, which provides more information that can be used to obtain search warrants, authorizations for surveillance, etc. This complex process is managed through a process known as One Vision 2.0, agreed upon by the Service and the RCMP.[64]

There remains, however, long-standing problems regarding challenges Canada faces in converting intelligence into court-ready evidence, known as the "intelligence-to-evidence problem." However, it clearly has an impact on national security investigations. For example, where CSIS s.21 warrants produce evidence of a crime which forms the basis of an RCMP investigation, the defence counsel may seek to challenge CSIS warrant in court, potentially jeopardizing the Service's sources and methods.[65]

Assistance Mandates: Importantly, departments and agencies like the CSE and DND/CAF may engage in domestic surveillance only when authorized to assist other departments and agencies, working under those agencies' legal mandates. For example, CSE may assist law enforcement or CSIS but only with the existence of appropriate legal authority. Where private communications are sought as a part of this assistance, a judicial warrant must be sought and provided to the CSE.[66]

When DND provides assistance, its authorities are the same as those governing the agency it is supporting.[67]

Collection Against Overseas Targets

<u>*CSE*</u>: Under the *CSE Act*, the organization is mandated to collect foreign intelligence, through the global information infrastructure on the government's intelligence priorities as set out in the NSPL discussed above.[68] The CSE does not have the authority to collect information on Canadians, unless authorized under its assistance mandate. However, given the nature of the internet (or "global information infrastructure"), it is likely that the Establishment will incidentally collect information on Canadians in the conduct of its foreign intelligence activities, some of which may implicate reasonable expectations of privacy. The risk is that this may infringe on s. 8 of the Charter, or Part VI of the *Criminal Code*. Therefore, the CSE Act allows for the Minister of Defence to issue a foreign intelligence authorization following an application by the Chief of the CSE. This application must demonstrate why they believe the collection of such data is necessary, reasonable, and proportionate; that information sought cannot reasonably be acquired by other means; and that any information that relates to Canadians or person in Canada will only be used, analyzed, or retained if essential to international affairs, defence, or security.[69]

Activities and classes of activities that a foreign intelligence authorization permits the CSE to engage in include:

> a) gaining access to a portion of the global information infrastructure;
> b) acquiring information on or through the global information infrastructure, including unselected information;
> c) installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting or intercepting anything on or through the global information infrastructure;
> d) doing anything that is reasonably necessary to maintain the covert nature of the activity; and
> e) carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activity, authorized by the authorization.[70]

Of note, under its *Act*, the CSE may carry out these activities following the foreign intelligence authorization, "despite any other Act of Parliament or of any foreign state." Some scholars note however, this conspicuously leaves out "international law."[71]

Importantly, once a foreign intelligence ministerial authorization is granted, the minister is required to provide a copy of the authorization to the intelligence commissioner. The intelligence commissioner has 30 days to review and determine whether the minister's authorization was reasonable; if it is, the Commissioner must approve it and provide written reasons for doing so.[72] The minister's authorization is only valid after this review and approval by the Intelligence Commissioner and only for a period of one year, although that may be extended for a second year without additional review.[73]

<u>*CSIS:*</u> Somewhat paradoxically, CSIS may collect foreign intelligence *within* Canada at the request of the Ministers of Foreign Affairs or Defence.[74] In practice, this means that CSIS may collect intelligence relating to the capabilities, intentions or activities of any foreign state or group of foreign states, or any person other than a Canadian citizen, a permanent resident, or Canadian corporation. As this collection takes place on Canadian soil, the use of intrusive means to collect the intelligence requires a s.21 warrant.[75] CSIS' international intelligence collection is strictly tied to its domestic security intelligence mandate (s. 12 of the *CSIS Act*) which allows it to investigate threats to the security of Canada as defined in s. 2 of the *Act*.

<u>*DND/CAF*</u>: As noted above, DND/CAF may collect overseas intelligence only where there is a nexus to its overseas missions – it is not an autonomous intelligence agency. However, there is no public standard or process for assessing when a "nexus" exists and it is often done on a "case-by-case basis."[76] As will be discussed below, there is no statutory authority for DND/CAF's intelligence activities, which are instead governed by a series of frameworks and directives.

V. RELEVANT LAW

Constitutional Provisions: The key constitutional instrument for individual rights is the *Canadian Charter of Rights and Freedoms*. Most relevant here is Section 8: "Everyone has the right to be secure against unreasonable search or seizure" (analogous to the American Fourth Amendment). Importantly, by design, *Charter* rights are not absolute. S.1 specifies that all *Charter* rights are guaranteed but subject to "such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."[77] In addition, the *Charter* has a "notwithstanding" clause, in s. 33 which allows Parliament or a provincial legislature to remove a statutory provision from Charter scrutiny for five-year renewable periods.[78]

Statutory Regimes: The major Canadian intelligence agencies have statutes which explicitly cover their activities. This includes the *Canadian Security Intelligence Service Act* and the *Communications Security Establishment Act*. In addition, the main review bodies are governed by statutes, including the I*ntelligence Commissioner Act,* the *National Security Intelligence Committee of Parliamentarians Act*, and the *National Security Intelligence Review Agency of Canada Act*.

Some departments and agencies do not have statutes which specifically govern their security and intelligence functions. DND/CAF is governed by the *National Defence Act*, but its intelligence activities are undertaken primarily under the authority of *Crown prerogative*. Crown prerogative is a source of executive power (usually the Prime Minister and the Cabinet) and privilege accorded by common law to the Crown, in circumstances in which the authority of the Crown is not otherwise limited (usually by statute, court decision or Constitution).[79] Guidance on the use and limitations of these powers are typically delineated in ministerial directives, some of which have been made public. For example, the *Ministerial Directive on Defence Intelligence*, issued under the defence minister's authority under the *National Defence Act*, sets out the governance framework for defence intelligence.[80]

For several years, government, military, and academic circles have debated whether DND/CAF's intelligence activities should be regulated by statue.[81] Those arguing in favour of the Crown prerogative note it is a long-standing and flexible source of authority and that the majority of the CAF's international operations are authorized under the Crown prerogative.[82] International deployments must be authorized by domestic law and be conducted in accordance with both Canadian and international law.[83] A NSICOP study on the issue found that the present framework needs clarification and that the Crown prerogative may provide sufficient legal authority for intelligence activities, particularly where they involve information about Canadians.[84]

Executive Orders or Decrees: In Canada, the Cabinet (also known as the Governor in Council) is the executive branch of government. As a part of exercising its powers, including appointments, and the implementation of powers or legislation, Cabinet will issue an "order in council" (OIC), which is a "legal instrument made by the Cabinet pursuant to a statutory authority or, less frequently, the royal prerogative."[85] Orders in Council are "made on the recommendation of the responsible Minister of the Crown and take legal effect only when signed by the Governor General."[86]

In the national security space, OICs are used to appoint individuals to review bodies such as NSICOP and NSIRA. Cabinet may also issue directions on how certain legislation must be implemented. For example, under the Avoiding Complicity in Mistreatment by Foreign Entities Act, Cabinet must issue directions to national security agencies, like CBSA and CSIS on handing information where information may result in mistreatment or inbound information may be

the product of mistreatment.[87]

Ministerial direction: As the executive branch of government, Cabinet ministers are given powers, duties, and functions by Parliament through statutes.[88] In exercising these powers, ministers will regularly issue directions (sometimes called *directives*), a written communication containing policy, procedures, instruction, or other information issued as an authoritative reference. For example, ministerial directives place certain obligations on the RCMP when it investigates terrorism or espionage cases, enters into agreements with foreign security or intelligence organizations to perform its national security functions, or investigates threats in "sensitive sectors" like universities.[89]

Agency Policies or Guidance Documents: As noted throughout this paper, all agencies and departments have their own policies and directives for interpreting ministerial directives, their mandates, and operations. For example, the procedures around CSIS' intelligence collection short of requiring a warrant refer to several guidance documents and policies that indicate who must be consulted or approve various targeting operations. Additionally, the CSIS dataset regime contains internal policies on who may have access to the information they contain. Unfortunately, most of these policies and guidance documents are not public. They may, however, be referred to in the reports of review bodies.[90]

Other Legal Instruments With Direct Effect in Domestic Law: Like other states, Canada is bound by both customary international law and treaties. Treaties are ratified through the executive (Cabinet) in Canada through an order in council. However, Canada views domestic law and treaty law as distinct. A treaty only has direct effect in domestic law after legislatures enact domestic legislation which effectively "transforms" the treaty into Canadian law.[91]

Canadian domestic law may have extraterritorial reach, but Canada tends to be conservative when extending its law beyond borders. Statutory law is not seen as extending beyond Canadian territory, with some exceptions outlined in the Criminal Code, including some terrorism laws. However, both criminal law and the *Charter* may follow government officials when they are overseas although the reach of the latter is debated. In addition, Canadian officials may not participate in activities, though authorized by the law of another state, that violate its international obligations in respect of human rights.[92]

VI. TRANSPARENCY

Although there has been an improvement in recent years (discussed further below), Canada's national security culture is opaque and lacking in transparency. A reasonable case can be made that Canada is the least transparent country within the Five-Eyes grouping.

As noted above, the powers and obligations of several national security and intelligence agencies have been placed into statutes in recent years. However, policies and procedures used by the Canadian national security and intelligence community remain unclear and often unavailable. This "secret law" includes ministerial directives, "memoranda of understanding, and internal policies and procedures which affect and govern the conduct of Canada's security agencies, but are excluded from the regular publication requirements for Canadian law."[93] Key agencies like the RCMP do not provide reports on their national security activities in the way that CSIS and the CSE do, and the public is provided little to no information on the regularity at which production orders, subscriber requests, or different kinds of electronic collection (such as IMSI catchers, malware, etc.) are used. Critics say Canada's poor system of reporting undermines legislators' abilities to hold the government to account and impedes outside researchers.[94]

Moreover, Canada's Access to Information and Privacy process is generally considered outdated, overly restrictive, and failing in its duty to make government more transparent.[95] Canada also lacks a declassification system, meaning that national security records are seldom released to the public, and not in any systematic fashion. There are no online or offline archives for historians and researchers to examine.[96]

Unlike other countries where there are regular (official and unofficial) communications between the national security community and the press, Canadian intelligence officials rarely give interviews or provide comment on news stories.[97] Additionally, Government of Canada websites are poorly organized, making it difficult to find information related to national security in an easy or systematic way. And when reports can be found, they often present information in inconsistent ways year on year, making it difficult to follow trends over time.[98]

Unlike other countries where there are regular (official and unofficial) communications between the national security community and the press, Canadian intelligence officials rarely give interviews or provide comment on news stories.

In 2017, the Trudeau government sought to address this issue through the creation of the National Security Transparency Advisory Group (NS-TAG). NS-TAG was given the mandate to advise the Deputy Minister of Public Safety Canada and the Government of Canada's federal departments and agencies with national security responsibilities on how to implement the National Security Transparency Commitment (NSTC).[99] This *Commitment* contains six principles related to improving the Canadian government's transparency in the area of national security related to information, executive and policy transparency.[100] Each year NS-TAG releases an annual report which discusses their work and their findings from interviews with government officials and community groups.[101]

At time of writing, NS-TAG is new and has been operating mostly in pandemic conditions. It is therefore hard to assess its success. However, it has already made contributions to developing and widening the concept of transparency in Canada.[102] In addition, some intelligence agencies, such as CSIS, have taken to publicly responding to their reports, including how it understands and plans to respond to NS-TAG's recommendations. This will hopefully create a constructive dialogue and plan for action.[103] A remaining challenge is increasing the demand for this information among Canadians, who are generally unfamiliar with Canada's national security agencies, despite seemingly having a high level of trust in them.[104]

VII. REFORMS

As a safe country, bordered by three oceans and a (normally) benign neighbour to its south, national security is seldom a pressing political issue in Canada. As such, legislators rarely bring forward legislation to update national security laws as there are few rewards for doing so. Instead, historically, national security legislation is normally brought forward in the aftermath of a scandal or crisis (like 9/11 or the 2014 Parliament Hill shootings), to which Parliament responds with omnibus bills consolidating various updates and reforms.

The result is that legal authorities are often out of date, in some cases better reflecting an era of fax machines than iPhones.[105] While CSIS and the CSE prefer clear lines for their activities, however, successive Canadian governments seem content with letting them operate in a sea of grey.

Nevertheless, there have been some important steps taken. Between 2016-2019, Canada underwent its most significant and comprehensive national security reforms since 1984. The Trudeau government, elected on a platform that included the substantial reform of Canadian national security law, brought forward two pieces of legislation: Bills C-22 and C-59.[106] These bills enhanced oversight and review of national security activities, better defined the activities of CSIS (especially its datasets regime) and empowered the CSE to take a more offensive cyber-security stance.

These reforms have brought Canada closer to its peers in terms of its ability to contribute to the security of the West and its allies, as well as in terms of the oversight and review powers of both parliamentary and statutory bodies. Many of these reforms are also due to be reviewed by Parliament in 2023 (five years after they came into force), which may result in further changes.

However, there are several areas where there remains a need for legislative reform. First, CSIS has been vocal about the need to modernize its authorities. While it has been vague about its specific modernization requests, it is generally understood that at least one relates to its concerns about the Service's ability to lawfully investigate ideologically motivated violent extremists (IMVE),[107] who tend to operate online and in loosely organized movements rather than specific groups. To what extent can the Service enter radical spaces online and look for threat-related behaviour without violating the meaningful expectation of privacy?[108]

A second issue is access to basic subscriber information (BSI). In 2014, the Supreme Court of Canada found that the method by which government agencies were obtaining BSI without a warrant unreasonably infringed on Canadians' Charter rights.[109] Multiple Canadian governments have sought to remedy this through legislation, but efforts have stalled. Officials accept that court authorization is necessary but note that the process to apply for a warrant for BSI (arguably the least intrusive warranted activity) is exactly the same as far more intrusive measures, such as conducting covert entries (the most intrusive power). In this sense the national security community is advocating an approach with more gradation based on the level of intrusion, rather than a "one size fits all" approach. Critics raise concerns about privacy and note that the problems Canada faces in this area have more to do with investigative capacity than legal gaps.[110]

Third, like other Five-Eyes countries, Canada is affected by the "going dark" debate with regard to encryption.[111] Generally, this debate has been less prominent than in the United States. However, national security agencies have expressed the need for lawful access to encrypted information to counter violent extremists' threats, particularly the RCMP who argue that Canada lags other countries in this area.[112] Critics point out that mandated "backdoors" to encryption tools will probably not fix systemic problems in criminal and national security investigations, and actually make the job of

organizations like the CSE (with their responsibility to protect government systems) harder.[113] At time of writing, it is not clear that there is a consistent position on the "going dark" issue that cuts across the Canadian national security and intelligence community.

VIII. OTHER IMPORTANT FACTORS

Overall, surveys suggest that Canadians continue to have trust and confidence in the national security and intelligence community – but very little familiarity with the agencies themselves. In 2018, only 30 percent of Canadians could name CSIS as the agency responsible for investigating threats to the security of Canada. Even worse, in 2020 only 3 percent of Canadians could name the CSE when asked which government agency is responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks.[114] Yet, despite the lack of familiarity with these organizations, the same surveys indicate that Canadians largely trust them, with large majorities expressing confidence in both CSIS and CSE.

Overall, surveys suggest that Canadians continue to have trust and confidence in the national security and intelligence community – but very little familiarity with the agencies themselves.

While the Canadian national security and intelligence community can take some satisfaction in these findings, it does not mean there is widespread support for increased levels of surveillance powers in Canada. Following the 2014 Parliament Hill shootings, the Stephen Harper government introduced sweeping legislation – some of which were likely unconstitutional.[115] While initially popular, once Canadians learned more about the legislation, support for it fell dramatically. For one of the few (if not first) times in Canadian history, national security legislation and surveillance became an election issue, with opposition parties running on platforms to repeal and/or reform the new national security powers.[116]

Ultimately, changes in both the international and domestic threat landscape may prompt national security concerns, and the role of surveillance, to a more prominent role in Canadian public affairs than has traditionally been the case. This includes IMVE threats, particularly in the aftermath of the Winter 2022 so-called "Freedom Convoy" movement, which challenged all levels of government in Canada. In addition, concerns about the long-term stability of its security alliances (including NATO and the Five Eyes) in an era of revisionist authoritarian powers, means that Canada may soon have to invest more in its own security. Whether or not Canadian politicians will break with tradition and act in this area, or if the Canadian public will support them in doing so, remains uncertain.

ENDNOTES

1. The author would like to thank Blaise Cathcart, Craig Forcese, Adam Klein, Philippe Lagassé, Christopher Parsons, Leah West, and anonymous others for their technical assistance in preparing this paper. All views in this paper are my own unless otherwise cited.
2. For more background on the Canadian intelligence and national security community discussed in this paper, see Stephanie Carvin, Thomas Juneau, and Craig Forcese, eds. *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*, Toronto: University of Toronto Press, 2021.
3. Canadian Security Intelligence Service Act (CSIS Act) R.S.C., 1985, c. C-23, https://laws-lois.justice.gc.ca/eng/acts/c-23/ (accessed May 11, 2023).
4. Terrorism or violent extremism is defined as "activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state." *Id.* at s. 2(c).
5. Communications Security Establishment Act (CSE Act), S.C. 2019, c. 13, s. 76 https://laws-lois.justice.gc.ca/eng/acts/C-35.3/page-1.html (accessed May 11, 2023).
6. For more on DND/CAF and CFINTCOM's intelligence functions, see Thomas Juneau and Stephanie Carvin, *Intelligence Analysis and Policy Making: The Canadian Experience*, Stanford: Stanford University Press, 2021. pp. 132-136.
7. Forcese and West, *National Security Law*, p. 456.
8. Forcese and West, *National Security Law*, p. 456.
9. *CSIS Act*, s. 16 (3); Forcese and West, *National Security Law,* p. 454.
10. *CSIS Act*, s. 21.1. Threat reduction measures are not surveillance activities (although they certainly rely upon surveillance) and thus will not be discussed here. For more, see Forcese and West, *National Security Law*, pp. 616-640 and Jez Littlewood, "Canadian Security Intelligence Service" in Stephanie Carvin, Thomas Juneau and Craig Forcese, eds. *Top Secret Canada: Understanding the Canadian Intelligence and National Security Community*. pp. 62-63.
11. *See* CSIS Act, s. 21.
12. Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism*, Toronto: Irwin Law Inc. 2015. pp. 362-363.
13. National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), S.C. 2017, c. 15, https://laws.justice.gc.ca/eng/acts/N-16.6/index.html (accessed May 11, 2023).
14. Philippe Lagassé, "Defence intelligence and the Crown prerogative in Canada", *Canadian Public Administration*, Vol. 64, No. 4, 2021. p. 544.
15. National Security Committee of Parliamentarians, *Special Report on the Collection, Use, Retention and Dissemination of Information on Canadians in the context of the Department of National Defence and Canadian Armed Forces Defence Intelligence Activities*, 2020, available at https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/special_report_20200312_public_en.pdf (accessed May 11, 2023).
16. National Security Committee of Parliamentarians, *Special report into the allegations associated with Prime Minister Trudeau's official visit to India in February 2018*, 2018, available at https://www.nsicop-cpsnr.ca/reports/rp-2018-12-03/intro-en.html (accessed May 11, 2023).
17. National Security Committee of Parliamentarians, *Annual Report 2020*, available at https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/intro-en.html (accessed May 11, 2023).
18. For more on this issue, see Philippe Lagassé, "Parliamentarians can be trusted with sensitive security information" *Globe and Mail*, 17 January 2022 available at https://www.theglobeandmail.com/opinion/article-parliamentarians-can-be-trusted-with-sensitive-security-information/ (accessed May 11, 2023); Leah West, Stephanie Carvin and Thomas Juneau, "National security can't become a tool of partisan feuding", *Globe and Mail*, 12 January 2022, available at https://www.theglobeandmail.com/opinion/article-national-security-cant-become-a-tool-of-partisan-feuding/ (accessed May 11, 2023); Intelligence Security Committee of Parliament https://isc.independent.gov.uk/ (accessed May 11, 2023).
19. National Security and Intelligence Review Agency Act (NISRA), S.C. 2019, c. 13, s. 2, available at https://laws-lois.justice.gc.ca/eng/acts/N-16.62/page-1.html (accessed May 11, 2023). In addition, NSIRA is mandated to investigate public complaints related to any activity carried out by CSIS and CSE, complaints relating to the denial or revocation of security clearances and complaints closely related to national security issues referred by the Civilian Review and Complaints Commission for the Royal Canadian Mounted Police (CRCC), matters referred by the Canadian Human Rights Commission (CHRC) and certain reports made to NSIRA under the Citizenship Act. NSIRA, "Complaints" https://nsira-ossnr.gc.ca/complaints. This may involve complaints about surveillance activities, but as it is not specifically related to surveillance, it will not be discussed in detail here.
20. National Security and Intelligence Review Agency, *Annual Report 2020*, available at https://nsira-ossnr.gc.ca/tabling-of-the-national-security-and-intelligence-review-agencys-annual-report (accessed May 11, 2023).
21. National Security and Intelligence Review Agency, *Review of CSIS Threat Reduction Activities*, November 2021, available at https://nsira-ossnr.gc.ca/review-of-csis-threat-reduction-activities (accessed May 11, 2023).
22. National Security and Intelligence Review Agency, *Review of the Communications Security Establishment's Disclosures of Canadian Identifying Information*, May 2021, available at https://nsira-ossnr.gc.ca/nsiras-review-of-cses-disclosures-of-canadian-identifying-information-cii (accessed May 11, 2023).
23. Martin L. Friedland, *Controlling Misconduct in the Military: A Study Prepared for the Commission of Inquiry into the Deployment of Canadian Forces in Somalia*, Ottawa: Minister of Public Works and Government Services Canada, 1997.
24. CSIS, "CSIS Internal Audit and Evaluation Branch / Disclosure of Wrongdoing and Reprisal Protection", 26 July 2021, available at https://www.canada.ca/en/security-intelligence-service/corporate/transparency/report-on-key-compliance-attributes-of-the-internal-audit-function.html (accessed May 11, 2023). When it was created in 1984, CSIS had an Inspector General office, described as the "eyes and ears" and "an early warning system" for the minister. The IG inspected CSIS' operational activities and therefore had both an oversight and review function. In a widely criticized decision, the Stephen Harper government abolished the IG office in 2012, claiming it would save $1 million CAD per year. *See also*, Forcese and Roach, *False Security*, p. 371.
25. The Privacy Commissioner evaluates federal government institutions' compliance with the Privacy Act and associated regulations. Much of the information collected through intelligence activities constitutes "personal information" under Canadian law. *See Privacy Act*, s. 3; *See also* National Security and Intelligence Committee of Parliamentarians (2020b, 13).
26. Forcese and Roach, *False Security*, p. 401.
27. Robinson, *Communications Security Establishment*, p. 78.
28. Julia Voo et al. National Cyber Power Index 2020, Harvard Belfer Centre, September 2020 available at https://www.belfercenter.org/publication/national-cyber-power-index-2020 (accessed May 11, 2023).
29. Bill Robinson, "Communications Security Establishment", *Top Secret Canada,* Toronto: University of Toronto Press, 2021. pp. 72-89. p. 75

30. Cabinet Committees are at the discretion of the Prime Minister and not enshrined by any statute. Though technically "ad hoc" they are not usually described or understood as such. See Prime Minister of Canada, Cabinet Committee Mandate and Membership, 3 December 2021, available at https://pm.gc.ca/en/cabinet-committee-mandate-and-membership (accessed May 11, 2023).
31. Insets include representatives of the Canada Border Services Agency (CBSA), CSIS and various provincial and municipal police services. Kent Roach, "Royal Canadian Mounted Police" in, Stephanie Carvin et al, *Top Secret Canada*, 130.
32. Maura Forrest, "Canada's national police force admits use of spyware to hack phones", *Politico*, 29 June 2022, available at https://www.politico.com/news/2022/06/29/canada-national-police-spyware-phones-00043092 (accessed May 11, 2023). Which companies the RCMP uses is not yet a matter of public record.
33. The laws regulating general search warrants that allow the police to conduct physical searches and seizures of property are found under s. 487 of the Criminal Code. Importantly, warrants to search a place do not authorize law enforcement to a place do not allow the police to search or seize electronic devices such as computers, laptops, tablets and smartphones which are seen as different kinds of "receptacles". Searches of these devices require a separate warrant and prior authorization (s. 487(2) of the Criminal Code). This authorizes police to not only search data contained within the devices, but also any information available to it through networked accounts and cloud-based systems. Forcese and West, *National Security Law*, pp. 415-416.
34. *Criminal Code*, s. 183; Interpretation Act s. 35 (1).
35. Forcese and West, *National Security Law*, p. 416; R v. Telus 2013, SCC 16 para 25.
36. Public Safety Canada, *Guidelines for Agents and Peace Officers designated by the Minister of Public Safety Canada*, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/gdlns-gnts-pc-ffcrs/index-en.aspx (accessed May 11, 2023).
37. Public Safety Canada, *Guidelines*; Forcese and West, *National Security Law*, p. 417.
38. Public Safety Canada, *Guidelines*; Forcese and Roach, *False Security*, p. 124; Forcese and West, *National Security Law*, p. 418. Part IV's judicial-approval provisions contain exceptions for emergency interceptions and situations where one party has consented to the collection and there is a serious risk of bodily harm. For example, in discussing its use of IMSI catchers, or "stingray" devices in Canada, the RCMP indicated in 2017 that all uses had authorization from a judge, except in one exigent circumstance in 2016. Dave Seglins, Matthew Braga and Catherine Cullen, "RCMP reveals use of secretive cellphone surveillance technology for the first time", CBC, 5 April 2017, available at https://www.cbc.ca/news/science/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750 (accessed May 11, 2023).
39. Public Safety Canada, *Guidelines for Agents*.
40. Forcese and West, *National Security Law*, p. 418. Public Safety Canada, *Guidelines*.
41. Forcese and West, *National Security Law*, p. 436. At time of writing, Canadian courts disagree about whether they have jurisdiction to issue production orders to companies that have only a virtual presence in Canada . *See id*., pp. 439-440.
42. Forcese and West, *National Security Law*, pp. 436-7. The complex nature of how emails are sent, received, and stored has raised questions as to whether there should be a specific provision in the Criminal Code in relation to how an e-mail should be acquired. See Public Safety Canada, "Interception of e-mail", in *Lawful Access - Consultation Document*, 7 September 2021 available at https://justice.gc.ca/eng/cons/la-al/d.html (accessed May 11, 2023).
43. Forcese and West, *National Security Law*, pp. 437-8; *Criminal Code*, s. 487.01(1)
44. *Criminal Code*, 487.015(1); Forcese and West, *National Security Law*, p. 438.
45. *Criminal Code*, 487.014 (1) and (2)
46. *Criminal Code*, 487.015 (1) and (2), 487.016 (1) and (2), 487.017 (1) and (2)
47. R v MacKenzie, 2013, SCC 50 at para 85.
48. Forcese and West, *National Security*, p. 438.
49. Criminal Code, 487 (2.1)
50. Forcese and West, *National Security Law*, pp. 415-6.
51. For more detail on CSIS targeting in counter-terrorism investigation, see Stephanie Carvin, "The Canadian Security Intelligence Service and the Toronto 18 Case", *Manitoba Law Journal*, Vol. 44, No. 1, 2021. pp. 97-114.
52. CSIS, *Internal Audit of Operational Compliance – Targeting*, (880-144), March 2013. Documents available through ATIP by Globe and Mail. See Colin Freeze, "CSIS Documents Reveal how Agency Designates Terrorism Targets," *Globe and Mail*, February 11, 2015, available at https://www.theglobeandmail.com/news/politics/csis-documents-reveal-how-agency-designates-terrorism-targets/article22905797/ (accessed May 11, 2023).
53. CSIS, *Internal Audit*, 1.
54. Carvin, "Canadian Security Intelligence Service", p. 108.
55. CSIS, *Internal Audit*, 4.
56. For matters that come under the *CSIS Act*, a "judge" refers to a judge of the Federal Court *designated* by the Chief Justice. Those participating in "designated proceedings" (the registry staff, amici curiae, special advocates, law clerks and government officials) all have security clearances and are subject to the *Security of Information Act*. Richard G. Mosley, "A View from the Bunker: The Role of the Federal Court in National Security", Lecture delivered at the Common Law Faculty at the University of Ottawa, 25 November 2015, available at https://www.fct-cf.gc.ca/Content/assets/pdf/base/Mosley%20J%20lecture%20-%20A%20View%20from%20the%20Bunker%20-%20for%20posting%20(ENG).pdf (accessed May 11, 2023).
57. Alternatively, in threat-to-life scenarios (such as the knowledge that an individual under investigation has access to a weapon and the intent to use it), the Service may inform the RCMP or other police service of an incident to prevent serious harm from occurring. While such an intervention may harm an investigation, the serious risk of a loss of life will trump operational concerns.
58. All legal services for the Canadian government are provided by the DOJ. This means agencies like CSIS and the CSE do not have their own lawyers but have DOJ lawyers embedded within their organizations. The rationale for this is to ensure departments and agencies are provide consistent legal advice across the government.
59. NSIRA, *Rebuilding Trust: Reforming the CSIS Warrant and Justice Legal Advisory Processes*, NSIRA Review 21-18. 16 June 2022, p.3, available at https://www.nsira-ossnr.gc.ca/wp-content/uploads/Review-arising-from-2020-FC-616-1.pdf (accessed May 11, 2023).
60. The definition of dataset has been deliberately left vague to accommodate a wide range of sources. The legislation does not preclude sources that have been purchased, voluntarily assistance, "walk-ins" or other more clandestine methods. The CSIS Act only governs dataset retention if it contains personal information (as defined in s.3 of the Privacy Act) and *does not* directly and immediately relate to activities that represent a threat to the security of Canada. Where a dataset directly relates to threat activities, retention is permitted under CSIS' more conventional legal authorities, if it is strictly necessary for the investigation.
61. Forcese and West, *National Security Law*, 428.
62. Forcese and West, *National Security Law*, p. 428.
63. In addition, datasets are available only to persons specially designated by the CSIS director. Every step of the process involving dataset and how they are used must be recorded, including the justification for queries. There is also periodic and random review by NSIRA. If NSIRA finds that a query or dataset did not comply with the law, it may refer the matter to the Federal Court.
64. Forcese and West, *National Security Law*, pp. 508-509.
65. Despite the centrality of the "intelligence to evidence" problem in Canada's national security investigations, and its impact on prosecutions, there is not the space to go into a full discussion in this paper on surveillance practices. For more information, see Forcese and West, *National Security Law*, pp. 465-468; Craig

Forcese, "Intelligence Swords and Shields in Canadian Law", 26 February 2018 (blog deactivated, entries on file with author). On the impact of this problem on CSIS electronic surveillance warrants specifically, see Forcese and West, *National Security Law*, pp. 664-666.
66. Robinson, "Communications Security Establishment", p. 77. Forcese and West, *National Security Law*, p. 91.
67. Forcese and West, *National Security Law*, p. 85. Of note, CSE has been criticized by NSIRA for its practices under its previous mandate (the National Defence Act) with regards to its procedures how its assistance to CSIS has been explained to the Federal Court, especially around providing Canadian Identifying Information to CSIS. CSE objected to the characterization of its practices in the NSIRA report, but reports that it has made unspecified changes to its internal policies and practices. NSIRA, Review of the Communications Security Establishment's Disclosures of Canadian Identifying Information, May 2021, available at https://www.nsira-ossnr.gc.ca/wp-content/uploads/2021/06/10397868-001-EN-CII-Review-2018-19-1.pdf (accessed May 11, 2023). See also the summary in Chris Parsons, NSIRA Calls CSE's Lawfulness Into Question, 18 June 2021, available at https://christopher-parsons.com/nsira-calls-cses-lawfulness-into-question/ (accessed May 11, 2023); Communications Security Establishment, *CSE Management Response to NSIRA Review of 2018-2019 Disclosures of Canadian Identifying Information*, 31 May 2021, available at https://nsira-ossnr.gc.ca/wp-content/uploads/2021/06/CSE-Management-Response-to-NSIRA-Review-of-Disclosure-of-CII_28-05-2021_English.pdf (accessed May 11, 2023). See also Catharine Tunney, "Cyber spies fall short on protecting Canadians' privacy after breaches, says new report", CBC, 5 March 2021, available at https://www.cbc.ca/news/politics/cse-privacy-nsira-1.5939001 (accessed May 11, 2023).
68. CSE Act, s. 16. In s.2 of the Act, "foreign intelligence" is defined as, "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security."
69. CSE Act s. 34 (1)-(2); Forcese and West, *National Security Law*, p. 451. Forcese and West note that this regime has not been tested in court as to whether it satisfies the Charter, but they believe it should. p. 453.
70. CSE Act, s. 26(2)
71. See testimony of Leah West, Proceedings of the Standing Senate Committee on National Security and Defence, Issue No. 41, Evidence – 29 April 2019, available at https://sencanada.ca/en/Content/Sen/Committee/421/SECD/41EV-54717-E (accessed May 11, 2023). In April 2022, Global Affairs Canada put forward its view of how international law applies in cyber space, which stated "…some cyber activities, such as cyber espionage, do not amount to a breach of territorial sovereignty, and hence to a violation of international law" but may violate national law. This is a similar position to that taken by the UK. Global Affairs Canada, *International Law applicable in cyberspace*, p. 19, 22 April 2022, available at https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng (accessed May 11, 2023);
Attorney General's Office (UK), "International Law in Future Frontiers", 19 May 2022, available at https://www.gov.uk/government/speeches/international-law-in-future-frontiers (accessed May 11, 2023).
72. Intelligence Commissioner Act, s. 20.
73. CSE Act, s. 36. The law also allows for emergency foreign intelligence authorizations. CSE Act, s. 40-1. Forcese and West, *National Security Law*, pp. 452-3.
74. CSIS Act, s. 16.
75. CSIS Act, s. 21. Forcese and West, *National Security Law*, pp. 454-455.
76. Forcese and West, *National Security Law*, p. 456.
77. Forcese and West, *National Security Law*, p. 45. As Forcese and West note, the Supreme Court of Canada has developed and articulated justification test for s. 1. In practice the "balancing" in s. 8 is done as a part of the "unreasonableness" assessment. Thanks to Craig Forcese for notes on this point.
78. However, this "notwithstanding" clause can only be used to limit the fundamental freedoms in s. 2, or the legal and equality rights in sections 7-15.
79. Peter W. Hogg, *Constitutional Law of Canada*, Toronto: Thomson Reuters Canada Limited, 2017; NSICOP, *Special Report*, pp. 9-10.
80. More granularity with regards to DND/CAF intelligence functions is provided in defence administrative orders and directives (DAODs) which are issued through deputy ministers and the chief of defence staff. This includes among others DAOD 8008-0, *Defence Intelligence* and DAOD 8002-2, *Canadian Forces National Counter-Intelligence Unit*. DND, DAOD 8002-2, *Canadian Forces National Counter-Intelligence Unit*, 2 June 2017, available at https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/8000-series/8002/8002-2-canadian-forces-national-counter-intelligence-unit.html (accessed May 11, 2023).
81. See Lagassé, "Defence intelligence"; Leah West, "The perilous prerogative: An argument for legislating defence intelligence in Canada", *Canadian Public Administration*, Vol. 65, No. 4, 2022. pp. 585-600.
82. The determination if an operation is in accordance with the law is determined by legal officers in the Office of the Judge Advocate General (JAG). These are all members in good standing of their respective provincial or territorial law societies and commissioned officers in the CAF. Moreover, Legal Officers from the JAG consult regularly with legal advisors from the Department of Justice, CSE and CSIS regarding the legal authority to conduct defence intelligence activities. Department of National Defence, *Judge Advocate General*, 11 June 2018, at https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/judge-advocate-general.html.
83. NSCIOP, *Special Report*, p. 9. The author thanks Philippe Lagassé for his discussion on this issue.
84. NSCIOP, *Special Report*, p. 45.
85. Government of Canada, "Orders-in-Council", 29 December 2021 available at https://www.canada.ca/en/privy-council/services/orders-in-council.html (accessed May 11, 2023).
86. *Id.*
87. Forcese and West, *National Security Law*, p. 495.
88. Prime Minister's Office, *Open and Accountable Government*, 27 November 2015, available at https://pm.gc.ca/en/news/backgrounders/2015/11/27/open-and-accountable-government (accessed May 11, 2023).
89. Forcese and West, *National Security Law*, pp. 645-650.
90. See for example, NSIRA, *Review of the Communications Security Establishment's Self-Identified Privacy Incidents and Procedural Errors*, 4 March 2021, available at https://www.nsira-ossnr.gc.ca/wp-content/uploads/2021/05/PIF_Report_Sept_2020_EN.pdf (accessed May 11, 2023). The report discusses the procedures for handling self-identified privacy incidents and procedural errors.
91. Forcese and West, *National Security Law*, pp. 36-38.
92. Forcese and West, *National Security Law*, pp. 39-42.
93. Craig Forcese, "Launch of 'Secret Law Gazette': Security Service Policies & Rule released under ATIP", 10 January 2017, and "Secret Law and Canadian National Security", 26 October 2016 (blog deactivated, entries on file with author).
94. Christopher Parsons and Adam Mohar, "Government Surveillance Accountability: The Failures of Contemporary Canadian Interception Reports," *Canadian Journal of Law and Technology*, Vol. 16, No. 1, 2018. pp. 143-169.
95. Sean Holman, "Canada's Access to Information Act is built to be broken", *Policy Options*, 8 November 2021, available at https://policyoptions.irpp.org/magazines/november-2021/canadas-access-to-information-act-is-built-to-be-broken/ (accessed May 11, 2023).
96. Andrea Conte, "Administrative sabotage", Briarpatch, 3 March 2022, available at https://briarpatchmagazine.com/articles/view/administrative-sabotage?utm_source=pocket_mylist (accessed May 11, 2023); Timothy Andrews Sayle and Susan Colbourn , "Canadians will be glad to know", *Policy Options*, 25 November 2021, available at https://policyoptions.irpp.org/magazines/november-2021/access-to-information-act-is-a-shambles/ (accessed May 11, 2023).
97. Alex Boutilier, "The Media and National Security Reporting in Canada", in Carvin, Juneau and Forcese, *Top Secret Canada*, pp. 274-281.
98. This has been a particular problem for the CSE which has refused to provide information about ministerial authorizations and has prevented NSIRA from reporting information about CSE's collection and sharing of private communications, information previously reported by a previous review body. Bill Robinson, *CSE 2020-2021 Annual Report, Lux Ex Umbra*, 9 December 2021, available at https://luxexumbra.blogspot.com/2021/12/cse-2020-2021-annual-report.html (accessed May 11, 2023).
99. Government of Canada, *National Security Transparency Advisory Group: Terms of Reference*, 22 December 2020, available at https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment/national-security-transparency-advisory-group/terms-reference.html (accessed May 11,

2023).
100. Government of Canada, *National Security Transparency Commitment*, 22 December 2020, available at https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html (accessed May 11, 2023).
101. See, for example NS-TAG, *National Security Transparency Advisory Group Initial Report: What We Heard in Our First Year*, 25 November 2020 available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-nstag-irwwh/2020-nstag-irwwh-en.pdf (accessed May 11, 2023).
102. NS-TAG, "The Definition, Measurement and Institutionalization of Transparency in National Security", 12 November 2021, available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-dntn-msrmnt-trsprncy-ns/index-en.aspx (accessed May 11, 2023).
103. CSIS, *CSIS Response to National Security Transparency Advisory Group (NS-TAG) Report*. 31 May 2022, available at https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-response-nstag.html (accessed May 11, 2023).
104. Discussed further in the conclusion.
105. 2016 FC 1105; see Jim Bronskill, "CSIS broke law by keeping sensitive metadata, Federal Court rules", CBC News, 3 November 2016, available at https://www.cbc.ca/news/politics/csis-metadata-ruling-1.3835472 (accessed May 11, 2023).
106. National Security and Intelligence Committee of Parliamentarians Act (NSICOP Act), (S.C. 2017, c. 15), and National Security Act, 2017 (S.C. 2019, c. 13).
107. CSIS uses IMVE to discuss what is often called "domestic extremism" in the United States and elsewhere.
108. Alex Boutilier, "Threats Within: Canada's spy service boosts attention to 'ideological' domestic extremism", *Global News*, 29 March 2021, available at https://globalnews.ca/news/8719009/threats-within-canadas-spy-service-boosts-attention-to-ideological-domestic-extremism/ (accessed May 11, 2023).
109. R vs Spencer [2014] 2 SCR 212, available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do (accessed May 11, 2023).
110. Christopher Parsons, *Lawful Access Returns: Online Harms and Warrantless Access to Subscriber and Transmission Data*, 3 February 2022, available at https://christopher-parsons.com/lawful-access-returns-online-harms-and-warrantless-access-to-subscriber-and-transmission-data/ (accessed May 11, 2023).
111. Lex Gill, Tamir Israel and Christopher Parsons, *Shining a Light on the Encryption Debate: A Canadian Field Guide*, Citizen Lab and The Canadian Internet Policy and Public Interest Group, 23 May 2018, available at https://cippic.ca/uploads/20180514-shining_a_light.pdf (accessed May 11, 2023); Leah West and Craig Forcese, "Twisted into knots: Canada's challenges in lawful access to encrypted communications", *Common Law World Review*, Vol. 49, Issue 3-4, 2020, available at https://doi.org/10.1177/1473779519891597 (accessed May 11, 2023).
112. RCMP, *Encryption and Law Enforcement,* 2016. Document accessed through The Canadian Internet Policy and Public Interest Group, available at https://cippic.ca/uploads/ATI-RCMP-Encryption_and_Law_Enforcement-2016.pdf (accessed May 11, 2023); Catherine Tunney, "RCMP issues dire warning about its ability to police terrorism, foreign interference and cybercrime", CBC, 12 March 2020, available at https://www.cbc.ca/news/politics/rcmp-significant-resourcing-challenges-security-1.5492424 (accessed May 11, 2023).
113. Tamir Israel and Christopher Parsons, "Government's encryption proposal will undermine public safety", *Toronto Star*, 28 August 2019 available at https://www.thestar.com/opinion/contributors/2019/08/28/governments-encryption-proposal-will-undermine-public-safety.html (accessed May 11, 2023).
114. Ekos, *Attitudes to the Canadian Security Intelligence Service (CSIS) – Baseline Study Final Report*, 12 June 2018, available at https://publications.gc.ca/collections/collection_2019/scrs-csis/PS74-8-1-2018-eng.pdf (accessed May 11, 2023); Pheonix SPI, *Attitudes towards the Communications Security Establishment – Tracking Study*, 30 April 2020., available at https://publications.gc.ca/collections/collection_2020/cstc-csec/D96-16-2020-eng.pdf (accessed May 11, 2023).
115. See, generally, Forcese and Roach, *False Security*.
116. Chris Hall, "Bill C-51: Political battle lines drawn over anti-terror bill as election nears", CBC, 19 February 2015, available at https://www.cbc.ca/news/politics/bill-c-51-political-battle-lines-drawn-over-anti-terror-bill-as-election-nears-1.2962764 (accessed May 11, 2023).