THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION V THE COMMUNICATIONS SECURITY ESTABLISHMENT OF CANADA[1]

PART I: INTRODUCTION

Our clients, the British Columbia Civil Liberties Association (the "**BCCLA**"), have brought a constitutional challenge against certain provisions of the *National Defence Act*[2] (the "***NDA***"). These provisions permit the Communications Security Establishment of Canada ("**CSEC**") to intercept, retain, and use the private communications of Canadians by obtaining a "**Ministerial Authorization**" from the Minister of National Defence (the "**Minister**"), rather than by obtaining a warrant from a court. CSEC also collects, stores, and uses metadata about Canadians without a warrant or any statutory oversight whatsoever.

In our claim, we argue that (among other things) CSEC's collection of the private communications of Canadians under Ministerial Authorization and its collection of metadata without any statutory oversight violate the *Canadian Charter of Rights and Freedoms* (the "***Charter***") s. 2(b), which protects freedom of expression, and s. 8, which protects against unreasonable search and seizure.[3] We focus on the s. 8 aspect of our claim for the purposes of this paper.

In its response to our claim, the government argues that CSEC needs the Ministerial Authorization procedure to protect its activities from disclosure and that comparable jurisdictions also rely on executive authorization regimes. The government further argues that its use of metadata has prevented attacks against Canadians and that CSEC needs this program to effectively identify and address cyber threats.

The government argues that its current regulations and procedures sufficiently protect the privacy of Canadians. The collection of Canadian communications does not, in the government's view, violate s. 8 of the *Charter* because it is authorized by the *NDA*; it is in furtherance of important government objectives; and it is minimally intrusive in terms of the type of information collected and in the sense that communications are subject to various privacy-protecting measures. The government puts significant weight on the fact that CSEC's activities are reviewed by the Commissioner of CSEC (the "**Commissioner**").

The government also argues that any infringement of the *Charter* is justified under *Charter* s. 1, which guarantees *Charter* rights but also allows the government to limit those rights if the limit can be demonstrably justified in a free and democratic society. CSEC has important objectives, including the protection of Canada and Canadians. The government says that CSEC's interception of private communications is rationally connected to its need to protect Canada's international affairs, defence and security interests, as well as Canada's IT infrastructure. It says that CSEC's measures are minimally impairing, in that CSEC conducts its activities "in a

[1] Joseph Arvay Q.C. and Alexander Boland of Farris LLP
[2] R.S.C. 1985, c. N-5
[3] *British Columbia Civil Liberties Association v. Canada (Attorney General)*, BCSC No. S137827, Vancouver Registry

tailored but technologically and practically feasible manner", subject to executive oversight and independent review by the Commissioner. Finally, it argues that the benefits of CSEC's activities outweigh any infringement of privacy or freedom of expression.

In this paper we begin by describing CSEC and the statutory framework under which it operates. We will explain why we object to the ministerial authorization process and assess the strengths of the government's arguments in favour of it. We will then discuss CSEC's metadata collection program, and why we think it is unconstitutional.

What is CSEC?

CSEC is an extremely secretive organization even within Canada's intelligence community. Its primary responsibility is the collection of foreign signals intelligence, but it also provides other Canadian government agencies with various information technology services. CSEC also at times assists other law enforcement agencies, such the Canadian Security Intelligence Service ("**CSIS**") and the RCMP, by conducting electronic surveillance on their behalf.

Founded in 1946 as the "Communications Branch of the National Research Council", CSEC formed after Canada began collecting signals intelligence alongside the United States, Australia, New Zealand, and the United Kingdom during World War II. The intelligence agencies of these countries continue to share intelligence today.[4]

CSEC is now administered by the Department of National Defence, and the Minister provides CSEC with high-level policy guidance by setting CSEC's intelligence priorities. The Minister also provides CSEC with general instructions on how it should carry out its activities: these instructions are known as "**Ministerial Directives**."[5] CSEC also issues its own policy manuals that provide detailed instructions to its operatives.

CSEC has a three-fold mandate, which is set out in s. 273.64 of the *NDA*. First, CSEC is tasked with the acquisition and use of information from the "global information infrastructure"[6] for the purpose of providing foreign intelligence in accordance with Government of Canada intelligence priorities ("**Mandate A**"). Second, CSEC provides advice, guidance, and service to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada ("**Mandate B**"). And third, CSEC provides technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties ("**Mandate C**").

The *NDA* prohibits CSEC from "directing" its Mandate A and Mandate B activities at Canadians.[7] Since Mandate C activities are carried out in conjunction with other law

[4] Communications Security Establishment "The Beginning: The Communications Branch of the National Research Council" (online: Communications Security Establishment) <www.cse-cst.gc.ca>; Communications Security Establishment "CSE's International Partnerships" (online: Communications Security Establishment) <www.cse-cst.gc.ca>.
[5] *NDA s.* 273.62(3)
[6] defined as including "electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or network."
[7] *NDA*, s. 273.64(2)(a)

enforcement or security agencies with their own procedural protections, CSEC may direct Mandate C activities at Canadians providing that the agency that CSEC is assisting has met its own procedural requirements.[8] So for example, CSEC may only conduct surveillance on behalf of the RCMP if the RCMP has obtained a warrant.

The *NDA* does not define what is meant by "direct", and so it is not clear the extent to which CSEC may deliberately target Canadians if it is ultimately aiming to recover obtain foreign intelligence. Potentially, CSEC could target Canadian citizens in Canada who are involved with, or who may be assisting, a foreign individual, state, organization, or terrorist group located outside of Canada in matters related to international affairs, defence or security and argue that the authorization is still "directed" at foreign entities in a broader sense.[9]

The secrecy under which CSEC conducts its activities makes it impossible to know whether or not it intentionally targets Canadians in this way. However, certain judicial comments suggest that CSEC may not legally target the communications of Canadians, even if its efforts are ultimately directed towards capturing foreign intelligence.[10]

The *NDA* also provides that Mandate A and Mandate B must be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.[11] The degree to which this provision actually protects Canadians is unclear.

CSEC's activities are reviewed by the Commissioner, who ensures that CSEC is complying with the *NDA*; the *Privacy Act*[12] and other relevant statues; and the *Charter*. The Commissioner is a supernumerary or retired judge, tasked with reviewing CSEC activities, investigating any complaints made against CSEC, and reporting to the Minister and the Attorney General any CSEC activity that the Commissioner does not believe to be in compliance with the law. The Commissioner also prepares annual reports both to the Minister and to Parliament that describe the Commissioner's activities, reviews, and findings.[13]

PART II: THE MINISTERIAL AUTHORIZATION SYSTEM

The first branch of our claim relates to the government's use of Ministerial Authorizations, which permit CSEC to collect the private communications of Canadians without a warrant.

A. What Are Ministerial Authorizations?

While CSEC may not "direct" its Mandate A and Mandate B activities at Canadians, the Minister may in certain circumstances authorize CSEC to intercept "private communications" in relation to an activity or class of activities. "Private communication" is defined in the *Criminal Code*[14] and means in simple terms any communication that is sent to or from Canada and that is made

[8] *NDA*, s. 273.64(3).
[9] R. Hubbard et al, *Wiretapping and Other Electronic Surveillance: Law and Procedure*, loose-leaf February 2014 update (Toronto, Ont.: Thomson Reuters Canada Limited, 2014) [Hubbard] ch. 17 at 2.1
[10] See, for example, *Canadian Security Intelligence Services Act (Can) (Re)*, 2013 FC 1275 at para. 106
[11] *NDA*, s. 276.64(2)(b)
[12] R.S.C. 1985, c P-21
[13] *NDA*, s. 273
[14] R.S.C. 1985, c. C-46

under circumstances in which the communicator had a reasonable expectation that the communication would not be intercepted.[15] So by obtaining a Ministerial Authorization, CSEC is able to intercept the private communications of Canadians, as long as that communication is either sent from or received in a foreign jurisdiction.

Unlike ordinary warrants, Ministerial Authorizations do not relate to specific individuals or specific crimes. Instead, Ministerial Authorizations authorize a particular activity or class of activities. By issuing a Ministerial Authorization, the government in effect sanctions a particular method of collecting intelligence.[16] In other words, Ministerial Authorizations may be like warrants that permits phone tapping at large, rather than the tapping of any particular phone.

The Minister may only issue a Ministerial Authorization under Mandate A if he or she is satisfied that:

1. the interception will be directed at foreign entities located outside Canada;

2. the information to be obtained could not reasonably be obtained by other means;

3. the expected foreign intelligence value of the information that would be derived from the interception justifies it; and

4. satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs.[17]

Similar requirements apply to Ministerial Authorizations that authorize CSEC to intercept private communications "for the sole purpose of protecting the computer systems of Canada from mischief, unauthorized use or interference" under Mandate B.[18]

The Commissioner must review activities carried out under Ministerial Authorizations to ensure that the activities are indeed authorized and legal. The Commissioner reports its findings annually to the Minister.[19]

Because Ministerial Authorizations relate to methods rather than particular investigations, CSEC requires very few Ministerial Authorizations. According to the government, between 2002 and 2102, CSEC applied for and received 78 authorizations, each relating to a particular method or activity. Many of these authorizations relate to the same class of activities in different time periods, since a Ministerial Authorization expires after a year (although they may be renewed). As far as we are aware, CSEC has never been denied an authorization it applied for. Nor are we aware of any situations in which the Minister granted a Ministerial Authorization on any terms other than those requested by CSEC.

---

[15] *Criminal Code*, s. 183
[16] *NDA*, s. 273.65(1)
[17] *NDA*, s. 273.65(2)
[18] *NDA*, s. 273.65(3)
[19] *NDA*, s. 273.65(8)

In its response to our claim, the Attorney General explained why CSEC intercepts "private communications" as follows:

> Despite the fact that CSE is directing its activities at non-Canadians outside Canada, in the relation to the Foreign Signals Intelligence Mandate, the complexity of the global information infrastructure is such that it is not possible for CSE to know ahead of time if a foreign target will communicate with a Canadian or person in Canada, or convey information about a Canadian. CSE's activities under its IT Security Mandate are directed at the acquisition of data, irrespective of its origin, that would potentially risk harm to the network being protected. As a result, the *National Defence Act* recognises that despite CSE targeting foreign entities, there may be circumstances in which incidental interception of private communications or information about Canadians will occur.

In other words, when CSEC targets communications that have "one end" in a foreign jurisdiction, it cannot always know ahead of time whether or not that foreign communicator will contact or be contacted by someone in Canada. As a result, it cannot be sure that it will not intercept private communications (communications to or from Canada). It therefore requires a ministerial authorization in order to give it legal authority to collect private communications incidentally intercepted.

The government tells us that these ministerial authorizations have captured only a "small" number of intercepted private communications, and that the CSE Commissioner reviewed each of the private communications so captured.

B. Why We Are Challenging The Ministerial Authorization Provisions

In our view, Ministerial Authorizations do not adequately protect the rights of Canadians. Canadian law requires that searches be authorized by persons capable of "acting judicially" and be based on clear legal standards. The Ministerial Authorizations fail to meet these criteria and are therefore unconstitutional.

While a detailed review of Canadian s. 8 jurisprudence is outside the scope of this presentation, the default thresholds for a reasonable (and therefore constitutional) search are clear. This threshold was set out by the Supreme Court in *Hunter v. Southam*.[20] Generally speaking, for a search to be reasonable the following criteria must be met:

1. a search warrant or other authorization must be obtained in advance of a search;

2. the authorization must be issued by a person "capable of acting judicially"; and

3. the authorization must only be issued after it has been established that reasonable and probable grounds exist to believe that an offence has been committed and that evidence is to be found in the place of search.

[20] [1984] 2 S.C.R. 145

Electronic surveillance such as wiretapping constitutes a search and is subject to the same analysis.[21] Indeed, the Supreme Court has noted that the importance of prior judicial authorization is even greater for covert interceptions of private communications, which constitute serious intrusions into the privacy rights of those affected.[22]

In certain circumstances, the government may engage in a search without prior authorization, but those circumstances are rare. One such exception is the regulatory context. In the regulatory context, the requirement for a search is based on a "sliding scale of reasonableness": this turns on the privacy interest engaged by the subject of the search and on the intrusiveness of the search itself. Where a search is highly intrusive and the individual's reasonable expectation of privacy in the subject matter of the search is high, the *Hunter* standards will continue to apply.[23]

Under a Ministerial Authorization, the government intercepts the private communications of Canadians. In our view, there can be little question that Canadians have a reasonable expectation of privacy in their communications, and this reasonable expectation exists even if the other party to the communication is located outside of Canada. The government's interceptions are not restricted to relatively anodyne information such as business records and do not relate to compliance with regulation. To the contrary, the government has indicated that it does not know in advance the subject matter of the communications it intercepts and so the government cannot itself assess the degree to which those communications involve private subject matters that can reveal the "biographical core" of the individuals whose communications are intercepted.

The government might argue that its search is relatively nonintrusive in that the individuals whose communications are intercepted do not even know that this interception has occurred. But this is true of any surreptitious collection of private communications, and such an approach belies the true danger of electronic surveillance. As the Supreme Court put it in *Duarte*:

> [I]f the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White*, *supra*, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.[24]

---

[21] See, for example, *R. v. Garofoli*, [1990] 2 S.C.R. 1421
[22] *R. v. Tse*, 2012 SCC 16 at para. 17
[23] *Arkinstall v. City of Surrey*, 2010 BCCA 250
[24] *Duarte* at 44

In other words, pervasive government surveillance threatens privacy precisely because it makes it impossible for any individual to have an expectation of privacy in any of his or her communications. As a result, interception of private communications is highly intrusive, even where it may be unclear to the communicators whether or not the government has in fact decided to intercept that particular communication. A government program wherein all communications that enter or leave Canada may be intercepted without any judicial oversight is, in our view, intrusive to an extreme degree.

The government might attempt to argue that it requires the ability to intercept private communications in order to protect Canada. We accept that in certain exigent circumstances the state may intercept private communications without meeting the standards set out in *Hunter*.[25] Part of CSEC's mandate involves collecting intelligence relating to terrorism and national defence, and in carrying out that mandate CSEC may, from time to time, encounter exigent circumstances that might justify a warrantless search although with the advent of tele-warrants we have a hard time accepting even that. Ultimately, there is no way for us to determine the frequency or degree of such exigent circumstances because CSEC does not provide any insight into its activities or the threats it claims to be combating.

Moreover, CSEC's interception of private communications under Ministerial Authorization is not limited to circumstances involving national security or defence, but also includes communications that relate merely to "international affairs."[26] This means that the government may intercept communications that have nothing to do with protecting Canadians, but rather simply are useful or desirable for the government as it carries out its international agenda. Given that in the past CSEC has infiltrated computers and smartphones affiliated with Brazil's mining and energy ministry, it is clear that CSEC's activities are not restricted to foiling terrorist plots or otherwise protecting Canadians.[27] We therefore do not think it can realistically be argued that all or for that matter any communications intercepted by CSEC are intercepted in exigent circumstances and therefore immune to the standard *Charter* analysis.

Further, to the extent that some of the information intercepted by CSEC may indeed relate to terrorism or national security, these communications fall closer towards law enforcement than they do regulatory compliance. Terrorism is, after all, a crime, and many activities that bear on national defence and foreign affairs may likewise have a criminal dimension. And in some circumstances CSEC will provide information to other Canadian government entities regarding violations of Canadian law; this disclosure may in turn lead to investigations and prosecutions.

Together, these factors lead us to conclude that CSEC's activities require the protections provided for in *Hunter*; CSEC is falling far short of these standards.

---

[25] See, for example, *R. v. Tse*, 2012 SCC 16

[26] *NDA*, s. 273.61

[27] C. Freeze and S. Nolen "Charges that Canada spied on Brazil unveil CSEC's inner workings" (October 7, 2013) online: The Globe and Mail< http://www.theglobeandmail.com/news/world/brazil-spying-report-spotlights-canadas-electronic-eavesdroppers/article14720003/>

1. Lack of Judicial Authorization

The most striking departure from *Hunter* is the fact that no judge ever authorizes a search made pursuant to a Ministerial Authorization, or even reviews the grant of a Ministerial Authorization after the fact. Instead, the Minister reviews the CSEC request and decides whether or not to grant an authorization. This is an apparent attempt to provide some of the protection of a warrant-like procedure, but it suffers from a fatal defect: the Minister cannot be considered a person "capable of acting judicially."

Section 8 does not require that all searches be authorized by a judge; in certain contexts, a search can be authorized by a non-judicial arbiter.[28] But whoever that arbiter is, he or she should be "capable of acting judicially." For example, in *Hunter* itself, the Court struck down ministerial search orders made under the *Combines Investigation Act*, party on the grounds that the minister is not a person capable of acting judicially.[29] In our view, the Minister's duties under the *NDA* and his or her portfolio make the Minister incapable of acting judicially.

The Minister's statutory duty under the *National Defence Act* is to manage and direct "all matters relating to national defence." The Minister therefore has an interest in favouring matters of security over the privacy and civil rights of citizens. The Minister is neither disinterested nor insulated from political pressures. The Minister cannot act as a neutral arbiter of CSEC surveillance requests, and therefore cannot act judicially.[30]

The government argues that the interests of national security justify the ministerial authorization structure. National security concerns do indeed give the government a certain amount of leeway when it comes to its ability to withhold disclosure of certain information to the general public.[31] The government will also argue that CSEC's activities are so sensitive that they must be protected as much as possible from disclosure. We see a number of flaws in these arguments.

In our view, it is not clear why CSIS should be required to seek judicial authorization, while CSEC can seek instead a Ministerial Authorization. Under its enabling act CSIS may intercept and retain information or intelligence on activities that may present a threat to the security of Canada.[32] But before doing so, CSIS must make an application to a judge of the Federal Court. This application must be accompanied by a sworn affidavit setting out reasonable grounds, investigative necessity, the type of communication to be intercepted, the identity of the persons to be intercepted, the targets of the interception, the places of the interception, and the period the interception: nearly the full gamut of procedural protections used in the law enforcement arena before obtaining a warrant.[33]

CSIS therefore has relatively stringent requirements along the lines of those provided for in *Hunter v. Southam,* yet nonetheless appears to be an effective part of Canada's security

---

[28] See, for example, *R. v. Simmons*, [1988] 2 S.C.R. 3, where the Court approved of a search procedure that was reviewed by a senior border officer

[29] *Hunter* at para. 32

[30] C. Forcese makes this argument in *National Security Law: Canadian Practice in International Perspective* (Toronto, Ont.: Irwin Law Inc., 2008) at 458

[31] *Hunter* at para. 43

[32] *Canadian Intelligence Services Act*, R.S.C. 1985, c. 23

[33] Hubbard ch. 17 at 8

intelligence community. If CSIS is capable of acting effectively through a judicial authorization procedure, there is no reason why CSEC could not also act effectively under a judicial warrant procedure. Likewise, there is no principled reason why CSEC requires greater secrecy or protection than does CSIS: both CSEC and CSIS engage in highly sensitive activities.

The experience of other nations also suggests that an appropriately tailored system of judicial authorization can work when applied to other organizations similar to CSEC. While many countries use some form of executive authorization,[34] some couple that executive authorization to judicial oversight.

For example, in the United States, when the government wishes to intercept the communication of persons located outside of the United States, the government must seek an authorization from both the Attorney General and the Director of National Intelligence under s. 702 of the *Foreign Intelligence Surveillance Act*[35] ("**FISA**"). Like Ministerial Authorizations under the *NDA, s.* 702 authorizations may not intentionally target individuals who are US citizens or residents, or who are physically located within the United State. But searches made under s. 702 may result in the incidental interception of communications to or from United States citizens or residents. Once an authorization is granted, the United States government may collect the communications of non-US persons in bulk and directly from service providers, including service providers in the United States.[36] Like Ministerial Authorizations, certifications do not apply to individual interceptions or targets, but rather to categories of foreign intelligence targets.[37]

After the executive grants an authorization under s. 702, the authorization is then reviewed by a neutral judicial body: the Foreign Intelligence Court, or "**FISC**." The FISC is a specialized body that operates largely in secret and with great sensitivity to national security concerns.

The Attorney General and Director of National Intelligence provide to the FISC a written certification and supporting affidavit that explains and justifies the authorization. The certification must attest that procedures are in place to limit targeting to persons located outside the United States; that appropriate minimization procedures are in place; that appropriate guidelines have been adopted; that a significant purpose of the acquisition of communications is to obtain foreign intelligence; and that the procedures in effect are consistent with the requirements of the Fourth Amendment.

These certifications are submitted annually to the FISC for review. The FISC then reviews the certification to ensure that the activities of the government fall within the standards set out by the legislation and by the court.[38]

The FISC also plays a direct role in setting the procedures in place for s. 702 searches. Each year, the FISC reviews the targeting and minimization procedures to ensure they satisfy all

---

[34] S. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham, Ont.: LexisNexis Canada Inc., 2005) at 231

[35] 50 U.S. Code § 1881a

[36] See generally R. Clarke et al, *Liberty and Security in a Changing World: Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies,* (December 12, 2014) online at whitehouse.gov, <whitehouse.gov> [*Liberty and Security*]

[37] *Liberty and Security* at 135

[38] 50 U.S. Code § 1881a

statutory and constitutional requirements.[39] In some respects, this role mirrors that of the CSEC Commissioner, but it departs from it in one important way: the FISC is not limited to making recommendations, but rather may issue binding rulings constraining the activity of government.

While the United States has yet to adopt a system of prior judicial review for the interception of foreign communications abroad, the United States has not sought to rely solely on executive and legislative oversight. Instead, certifications are reviewed by the FISC. Further, the procedural safeguards in place are also approved of by the FISC. This is a clear indication that the path chosen by Canada - which provides for no judicial role whatsoever - is not the least restrictive option available to government.

Of course, the FISC is not without criticism, often on the basis that it approves the vast majority of warrant applications brought to it: over 99% of warrant applications are approved. This has resulted in many arguing that the FISC is merely a "rubber stamp" that exists to legitimize intrusive government actions.[40]

The same concern might be leveled at the Federal Court in its review of CSIS warrant requests, which it very rarely denies.[41] The Federal Court nonetheless provides an important role in reviewing CSIS searches. Rather than acting merely as a "rubber stamp", the Federal Court ensures that CSIS acts within its statutory authority and takes seriously its *Charter* responsibilities.

For example, in *X (Re)*[42] the Mr. Justice Mosley rebuked both CSIS and CSEC for failing to act with due candour during *ex parte* warrant proceedings.

CSIS had first sought a warrant permitting it to undertake certain investigative activities outside of Canada; that request was refused by Blanchard J., as he considered that the court lacked jurisdiction to authorize searches outside of Canada. In a second application (this time before Mosley J.), CSIS sought a warrant to intercept foreign communications by employing CSEC under its Mandate C. This second application succeeded, as CSIS assured the court that the actual interception would take place wholly within Canada. The court held that it had jurisdiction to regulate the activities of Canadian intelligence organizations when operating within Canada.

Mr. Justice Mosley later learned that in the second application CSEC and CSIS had deliberately and strategically hidden from the Court key information that CSIS had presented to Blanchard J. in the first application: much of the interception was not carried out by CSEC at all, but rather through the assistance of Canada's "Five Eyes" allies. Mr. Justice Mosley delivered a stinging rebuke to CSEC and CSIS, and stressed that the Court's jurisdiction did not permit CSIS to request that foreign intelligence agencies intercept the communications of Canadian persons either directly or through the agency of CSEC under its Mandate C.[43]

---

[39] 50 U.S. Code § 1881a

[40] See, for example, Conor Clarke "Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp? Ex Parte Proceedings and the FISC Win Rate" (2014) 66 Stan. L. Rev. Online 125[Clarke] at 125 note 2

[41] For example, in 2006-2007 it approved 176 warrants and denied none. Security Intelligence Review Committee, *SIRC Annual Report 2006-2007* (Ottawa, Ont.: Public Works and Government Services Canada, 2007) at 52-53

[42] 2013 FC 1275

[43] *X (Re)* at paras. 116-126

X (Re) illustrates that even courts that tend to generally approve government warrant requests play an important role in checking government misconduct. It also illustrates that intelligence agencies cannot be left to determine for themselves the boundaries of their actions. Far from acting as "rubber stamps", national security courts ensure that intelligence agencies act within the law and with appropriate regard for constitutional rights.

Another frequent criticism of the FISC is that it operates largely *ex parte*, with the sole party before it being the government. Indeed, one former member of the FISC, Judge Robertson, has advocated for the introduction of an adversarial hearing into the FISC process:

> I have no problem with ex parte proceedings to approve individual warrants. Judges and magistrates do that every day. Where I draw the line is with the notion that precedents are being set, and followed, ex parte, or that ex parte proceedings are being conducted for the approval of programs. Program review, it seems to me, is like review of administrative agency actions. Judges do that, but never ex parte. Anybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding. It's quite common – in fact it's the norm – to read one side's brief or hear one side's argument and think, hmmm, that sounds right. Until we read the other side. Judging is choosing between adversary positions.
>
> That is why I have advocated, and why a number of senators and congressmen have proposed legislation that would allow or require adversary proceedings at the FISA court.[44]

For this reason, some have suggested that the FISC adopted an "amicus" program wherein security-cleared lawyers would argue on behalf of the public as a way of checking government.[45] We think that if CSEC were to seek judicial authorizations prior to intercepting Canadian communications, the employment of an *amicus* would make sense and would be consistent with other Canadian security procedures, such as the "special advocate" provisions under the *Immigration and Refugee Protection Act*[46] (although we hasten to note that these provisions are themselves problematic in various respects). Indeed, the federal court already appoints *amici* in carrying out its review of CSIS warrant requests.[47]

Ultimately, while CSEC may have particularly acute secrecy and national security concerns, there does not appear to be any reason why CSEC could not effectively achieve all of its goals while also respecting the privacy of Canadians through the use of effective safeguards, including and especially judicial oversight. CSEC is already subject to some review by the Minister and the Commissioner, and putting that oversight into the hands of judges would not appear to dramatically alter anything about CSEC's day-to-day operations. Finally, the example of CSIS

---

[44] Judge James Robertson, "Intelligence, Surveillance, and the Courts" (Speech delivered at the American College of Trial Lawyers Conference, October 2013) [unpublished]

[45] A. Nolan and R. Thompson, "Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Changes" (January 16, 2014) Congressional Research Services at 9-16

[46] S.C. 2001, c. 27, ss. 85-85.6

[47] See for example *Canadian Security Intelligence Service Act (Re)*, 2008 FC 300, where Ron Atkey, Q.C., was appointed *amicus*

and the United States provides proof that judicial authorization and review is consistent with the activities of spy agencies such as CSEC.

2. Lack of a Clear Legal Standard

The Ministerial Authorizations depart from traditional warrants in the legal standards required of the minister before an authorization is issued.

The *NDA* limits Ministerial Authorizations to circumstances where the Minister is satisfied that the interception will be directed at foreign entities located outside Canada; that the information to be obtained could not reasonably be obtained by other means; that the expected foreign intelligence value of the information that would be derived from the interception justifies it; and that satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs. However, the *NDA* does not explain what standard applies to these considerations. In conventional warrant applications, that standard is reasonable grounds. It is not clear whether the same standard applies to Ministerial Authorizations, and if it does not, what standard should be applied instead.

Commissioners have raised concerns regarding the ambiguity in terms of legal standard and have repeatedly recommended that the *NDA* be amended to clarify the standard that applies to the preconditions for a Ministerial Authorization and to clarify whether the terms of the *NDA* permit broad, method-based Ministerial Authorizations; these recommendations have not been heeded and the NDA remains in its original, suspect form.[48]

This lack of particularity is especially concerning given the extreme breadth of the activity authorized by a Ministerial Authorization. Rather than being particular to any particular person, communication, or even subject matter, Ministerial Authorizations authorize a specific <u>method</u> of acquiring foreign signals intelligence.

The scope of a "specific method" is unclear - while the government has disclosed Ministerial Authorizations, they have uniformly been redacted to the extent that the nature of the activity authorized cannot be ascertained. However, the fact that CSEC requires only a few Ministerial Authorizations each year suggests that the scope of the activities described in the Ministerial Authorizations is broad indeed. Further, CSEC appears to be combining different activities that were formerly subject to different Ministerial Authorizations into a single Ministerial Authorization in a process of "harmonization."

Given the generality of the Ministerial Authorizations, it is also not always clear whether the preconditions of a ministerial authorization are in fact being met. In his 2005-2006, Commissioner Lamer (as he then was) noted this problem, stating that:

---

[48] See Communications Security Establishment Commissioner, "Annual Report 2006-2007" (Ottawa: Minister of Public Works and Government Services Canada, 2007) at 2-3; Communications Security Establishment Commissioner, "Annual Report 2007-2008" (Ottawa: Minister of Public Works and Government Services Canada, 2008) at 3-6; Communications Security Establishment Commissioner, "Annual Report 2008-2009" (Ottawa: Minister of Public Works and Government Services Canada, 2009) at 2-3; and Communications Security Establishment Commissioner, "Annual Report 2009-2010" (Ottawa: Minister of Public Works and Government Services Canada, 2010) at 3-4

> [R]eviews completed by my office, including the most recent one, have shown that supporting documentation provided by CSE as part of requests for the Minister's authorization address the underlying foreign intelligence requirements only in general terms. The lack of clarity in this regard has made it difficult for my staff to assess compliance with certain of the conditions that the legislation requires to be satisfied before a ministerial authorization is given.[49]

The lack of a clear legal standard further undermines the reasonableness of CSEC's ability to intercept the communications of Canadians.

3. The Commissioner Is Not a Sufficient Safeguard

An existing check on CSEC's power - and one relied on by the government in its reply to our claim - is the Commissioner of CSEC.

As described above, the Commissioner is a former or supernumerary judge who is made responsible for monitoring CSEC compliance with the law and the *Charter*. The Commissioner reviews the interception of private communications to ensure legal and constitutional compliance, as well as compliance with the terms of the enabling Ministerial Authorization.

While we concede that the existence of the Commissioner is better no oversight at all, we do not believe that the Commissioner is an adequate replacement for a process of judicial authorization and review.

First, the Commissioner has no enforcement mechanism. While the CSEC commissioner reports to the Minister and, on an annual basis, to Parliament, the CSEC commissioner cannot force CSEC to comply with the law. The Commissioner can only make recommendations, and CSEC is under no obligation to accept those obligations.[50] In circumstances where CSEC behaves unconstitutionally but does so with the approval of the government and Parliament, the CSEC Commissioner is wholly unable to act as a check on CSEC's power. If one of the purposes of a warrant is to protect the powerless and unpopular from coercive treatment by government, the Commissioner is sadly lacking.

Second, the Commissioner is to some degree dependent on the cooperation of CSEC. While the Commissioner has generally reported that CSEC is currently cooperating with the Commissioner, we have no assurance that this will always be the case. Further, since we have no access to the inner workings of the Commissioner the public has no way of gauging whether the Commissioner's review is appropriately thorough or effective. Finally, we note that - given its secretive nature - CSEC is likely quite capable of hiding any misconduct from the Commissioner.

---

[49] Communications Security Establishment Commissioner, "Annual Report 2005-2006" (Ottawa: Minister of Public Works and Government Services Canada, 2006) at 10

[50] Between April 1996 and March 2006, roughly 25% of the Commissioner's recommendations went unheeded by CEC: S. Lefebvre, "Canada's Legal Framework for Intelligence" (2010) 23 International Journal of Intelligence and CounterIntelligence 247 at 262

Third, the Commissioner only reviews authorizations after the fact. Post-facto review can at best produce recommendations for the future, but cannot prevent abuse before it occurs and cannot provide any relief to those whose rights have been infringed. Prior authorization provides an opportunity for the conflicting interests of the state and individual to be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are demonstrably superior.[51] This is not the case where any review is after the fact.

PART III: COLLECTION AND ANALYSIS OF METADATA

A second dimension of our claim relates to CSEC's collection and use of metadata. Our position is that metadata is no different in principle than other forms of communication. Consequently, we argue that before collecting metadata, the government should be required to obtain judicial authorization.

A. What is Metadata and What is CSEC Doing With It?

Metadata is information that describes a communication. Metadata includes email addresses, phone numbers, geolocation information, the time a communication was sent or received, the identity of the sender or recipient of information, and practically any other piece of information relating to a communication, other than the content of the communication itself.

Metadata can be highly revealing. The fact that a person (for example) telephones an abortion clinic reveals detail private information about that person. If a government were to collect all metadata about a person, the government could determine who a person communicated with; where a person lived and worked; with whom the person associated; and what websites a person visited. By combining these details together, the government could created a detailed profile of a person's life, convictions, and habits.[52] Consequently, a former NSA General Counsel stated "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[53]

Further, because metadata is relatively simple information (often just strings of numbers), it can be combined and analyzed in a way that the contents of a communication cannot. Computer programs can more easily analyze sets of numbers that describe communications - like time and place of a phone call—than the complexities of an actual human conversation. So it is not only possible for the government to combine metadata in a way that reveals important and private information about individuals, it is actually practical for it to do so.[54]

The government admits that it collects metadata, and it is clear from its response and its disclosure that this includes the metadata of Canadians. Unfortunately at this time we have no clear information on what kinds of metadata CSEC is collecting, where it is obtaining that

---

[51] *Hunter* at para. 32

[52] C. Forcese "Law, Logarithms and Liberties: Legal Issues Arising from CSEC's Metadata Program (Working Paper)" (2014) online at Social Science Research Network <papers.ssrn.com> [Forcese (2014)] at 4-5

[53] S. Landau, "Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations" (July/August 2013) 11 IEEE Security & Privacy 54 [Landau] at 62-63

[54] Forcese (2014) at 5

metadata, and what it is doing with it once it has got it. We have some information that we received through the discovery process but we are constrained from disclosing that in this paper because of the implied undertaking rule. There are no Legislative Checks on CSEC's Metadata Activities.

One of our central concerns is the fact that CSEC's metadata collection and analysis takes place entirely outside of any specific legal constraint. CSEC does not consider metadata to constitute private communications, and so it considers itself entitled to collect and analyze metadata not just without a warrant, but also without a Ministerial Authorization or even a Ministerial Directive. While the Minister has issued various policies and directives relating to metadata activity, the Minister is not under any obligation to do so.

At this time, the only existing legislative protections that apply to metadata are the general terms of the *NDA*, including: the admonition in the *NDA* that CSEC must act within its Mandates, Ministerial Authorizations, and Ministerial Directives[55]; the provisions in the *NDA* preventing CESC from directing its activities at Canadians,[56] and the provisions requiring CSEC to subject its activities to privacy-protection measures.[57] These general provisions are not an adequate substitute for a system of prior authorization.

In its response to our claim, the government argues that "any metadata related activities are also subject to applicable Ministerial directives, applicable Ministerial authorizations and various other policies and procedures put in place to provide comprehensive protection for the privacy of Canadians and persons in Canada." The government has provided us with some of the documents outlining these policies and procedures, but has redacted them so heavily we can draw very few conclusions regarding the specifics or extent of the policies. Again we are constrained to say any more about that given the implied undertaking rule.

The government argues that metadata does not constitute "private communication" for the purposes of the *NDA* and that metadata does not attract s. 8 protection. As a result, it will argue that it need not seek a warrant nor a ministerial authorization.

Our view is that the Supreme Court of Canada's judgment in *R. v. Spencer* clearly establishes that metadata reveals private information in a way that can engage s. 8 of the *Charter*.[58]

In *Spencer*, the defendant had shared child pornography with others over the internet. The police were able to obtain the defendant's IP address (a series of numbers that identifies a particularly internet connection). While the Supreme Court did not describe it in these terms, the defendant's IP address is metadata: it is data that describes the defendant's network connection. The defendant's IP address revealed that his computer was likely located in Saskatoon and that his internet connection was provided by Shaw, but it did not reveal his name or address. The police wrote Shaw directly, asking them for the personal information of the subscriber associated with the IP address, including the subscriber's name, address, and telephone number. The police used this information to locate and arrest the defendant.

---

[55] *NDA*, s. 273.66
[56] *NDA*, s. 273.64(2)(a)
[57] *NDA*, s. 273.64(2)(b)
[58] 2014 SCC 43

According to the Supreme Court of Canada, the defendant had a privacy interest in his IP address. By seeking to associate that IP address with a particular identity, the police had engaged in a search. By reaching this conclusion, the Court recognized that the superficially "mundane nature" of metadata can belie its ability to reveal intimate details of the lifestyle and personal choices of the individual to whom it relates.[59] The importance of the metadata in question reflected its capacity to reveal important personal details once it was associated with identifying information.[60]

The court also noted that by stripping the defendant of anonymity, the search implicated the defendant's privacy in a broad and substantive way. Subscriber information that links particular kinds of information to identifiable individuals implicates interests relating not simply to the person's name or address but to his or her identity as the source, possessor or user of that information. In other words, such a link reveals the fact of a person's identity, but also their interest in a particular kind of information.[61] This linking of identity to information engages a high level of privacy interest.[62]

We cannot overstate *Spencer's* importance. As one commentator put it, "The Supreme Court is prepared to extend s. 8 protections to the most benign data - name and address and telephone number - associated with an IP address and which everyone appreciates a telecommunication company collects for billing purposes."[63] And if that is the case, *a fortiori* constitutional protection ought to extend to the potentially more intimate forms of metadata that CSEC may be collecting.

That being the case, CSEC's position that metadata cannot constitute "private communication" and that it can collect all metadata without even the sanction of a Ministerial Authorization is likely untenable. The Supreme Court of Canada has indicated that at least some kinds of metadata attract s. 8 protection. As a result, the government should be required to obtain a warrant before collecting or searching metadata.

We suspect that the government has a reason to assert that metadata is not a private communications. It may be that CSEC's current activities using metadata would not be legal were they to be considered private communications, even with a Ministerial Authorization. For example, the *NDA* prevents CSEC from targeting the private communications of Canadians, with or without a Ministerial Authorization. If metadata is can constitute private communications, then CSEC would be forbidden from deliberately collecting that information. We suspect that CSEC is indeed deliberately collecting the metadata of Canadians: if this metadata is private communications, then CSEC's activities in that regard are unlawful.

---

[59] *Spencer* at para. 25
[60] *Spencer* at para. 32
[61] *Spencer* at para. 47
[62] *Spencer* at para. 51
[63] C. Forcese, "Why Spencer Changes the Playing Field for CSEC & National Security Spying" (June 17, 2014), online: National Security Law <http://craigforcese.squarespace.com>

B. US Procedure For Metadata

Before closing, we will consider in brief the United States' procedure for metadata collection and analysis. While hardly a paragon of transparency or moderation, we do note that the US metadata collection program at least takes place under some degree of judicial supervision. We further note that since the United States has been able to implement an apparently effective and extremely wide ranging metadata program while retaining judicial supervision, any argument on the part of CSEC that judicial supervision would render its activities impracticable should be given little weight.

Thanks to the revelations made by Edward Snowden, the world has learned with a certain amount of detail the nature and extent of American metadata programs. Following these revelations, the United States government has explained in further detail the procedures and legal protections in place when it comes to at least some of its metadata-related programs.

One of these programs is the "telephony metadata program", through which United States government requires telecommunications companies to produce "telephony metadata" (i.e. phone records) in bulk [64] This metadata includes information about what telephone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted. The government analyzes this information to determine whether known or suspected terrorist operatives have been in contact with other persons who may be engaged in terrorist activities. This practice of "contact chaining" allows the government to uncover networks of relationships.[65]

The United States government asserts that its telephony metadata program is authorized under s. 215 of the Patriot Act.[66] In order to obtain metadata from telecommunications companies, the FBI must obtain an order from the FISC. The government's application must include a statement of facts that shows there are reasonable grounds to believe that the records sought are relevant to an authorized investigation into terrorism. The basic position of the FBI is that it must obtain all telecommunications records in order to practice contact chaining and other analysis within those records. In the government's view, all telecommunications records are therefore "relevant" to an investigation. While this understanding of relevance is far from uncontroversial, the FISC accepts it and in 35 subsequent decisions has repeatedly ordered telecommunications providers to turn over to the government on an ongoing basis all telephony metadata created by communications between the United States and abroad, or wholly within the United States. [67]

But the FISC has not acted simply as a rubber stamp. Instead, it has imposed a number of additional procedural protections not found in the text of s. 215 itself. For example, the government must store and process meta-data in secure government repositories and restrict

---

[64] See generally *Liberty and Security*; Administration White Paper, " Bulk Collection of Telephony Metadata Under S. 215 of the USA Patriot Act" (August 9, 2013) online <http://perma.cc/8RJN-EDB7> [White Paper]

[65] White Paper at 1

[66] The government asserts the program's legality, although this remains a matter of controversy among commentators and some judges; see for example CJ. McGowan, "The Relevance of Relevance: Section 215 of the USA Patriot Act and the NSA Metadata Collection Program" (2014) 82 Fordham L. Rev. 2399 [McGowan].

[67] White Paper at 8-15; for a critique of this reasoning see "Recent Administration White Paper" (2014) 127 Harvard L. Rev. 1871

access to authorized and trained personnel; the government is prohibited from accessing the metadata for any purpose other than to obtain foreign intelligence information; the government may only search the metadata if it has a reasonable, articulable suspicion that a specific selector (i.e. telephone number) is associated with a specific foreign terrorist organization; and the FISC must review and approves the list of specific foreign terrorist organizations to which all queries must relate. Only 22 people in the NSA can give approval to search metadata, and any approval has to be independently approved by two of these people, then approved by a supervisor.[68] While the FISC does not approve individual searches of the metadata repository, it receives reports every 30 days on the number of selectors (i.e. phone numbers) used to query the metadata and the results of those queries.

The safeguards used in the United States are superior to any policy adopted by CSEC in one crucial respect: the safeguards created by the FISC have the force of law. The FISC can and does ensure that the program is operated with due respect for individual rights. For example, in 2009 a FISC judge found serious problems in the metadata program: procedural protections had been frequently and systematically violated, albeit unintentionally. In particular, many of the identifiers used to query the database did not meet the "reasonable, articulable suspicion standard." As a result, the FISC altered the s. 215 order to permit the government to access the database only subject to a FISC order authorizing a specific query "on a case-by-case" basis, and only after the FISC itself found that a reasonable articulable suspicion exited. While this restriction has been lifted, it shows that the FISC can act as an effective safeguard of individual rights.[69]

This model is far from perfect, and has resulted in the bulk collection of massive amounts of information about Americans and non-Americans. The practical benefits of this information are unclear, and it is somewhat in doubt whether these bulk collection programs significantly assist counterterrorism efforts in the first place.[70] A variety of proposals have been suggested to reform the system, at least as far as collection of information about Americans' goes. These suggestions include higher standards for collection as well as increased judicial review and an FISC approval process for the search of collected data.[71]

Moreover, there continues to be debate over whether the limited protections protection provide by the FISC are enough to render s. 215 constitutional. For example, in *Klayman v. Obama*, Judge Richard Leon of United States District Court for the District of Columbia held that the provisions of s. 215 likely violated the Fourth Amendment.[72] In *Klayman*, the plaintiffs sought a preliminary injunction that would bar the government from collecting the plaintiffs' phone records; require the government to destroy existing call records; and prohibit the government from querying existing records using data associated with the plaintiffs. Since *Klayman* was an injunction application, the plaintiffs needed only to show that they had a substantial likelihood of success on the merits. Judge Leon concluded that the plaintiffs had met that standard, stating:

---

[68] Liberty and Security at 97-102
[69] Liberty and Security at 105-106
[70] Landau at 59-60
[71] McGowan at 2433 and 2435
[72] 3024cv0851-48

> The Fourth Amendment typically requires "a neutral and detached authority be interposed between the police and the public," and it is offended by "general warrants" and laws that allow searches to be conducted "indiscriminately and without regard to their connection with [a] crime under investigation." *Berger v. New York*, 388 U.S. 41, 54, 59, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967). I cannot imagine a more "indiscriminate" and "arbitrary invasion" than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval. Surely, such a program infringes on "that degree of privacy" that the Founders enshrined in the Fourth Amendment. Indeed, I have little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgement of freedom of the people by gradual and silent encroachments by those in power," would be aghast.[73]

But in *ACLU v. Clapper*, the United States District Court for the Southern District of New York reached the opposite conclusion.[74] In *Clapper*, the plaintiffs sought a declaration that the s. 215 metadata collection program violated the Fourth Amendments. Judge Pauley found that it did not, relying heavily on the U.S. Supreme Court case *Smith v. Maryland*.[75] In *Smith*, the Supreme Court held that individuals have no "legitimate expectation of privacy" in the telephone numbers they dial because they knowingly give that information to telephone companies whenever they dial a number. In Judge Pauley's view, telephony metadata - comprised of call records compiled and maintained by telephone companies - belonged to the telecommunications companies rather than the plaintiffs and so the plaintiffs had no privacy interest it in. Accordingly, the s. 215 program did not violate the Fourth Amendment.[76]

Perhaps unsurprisingly, the FISC itself has considered and rejected Judge Leon's reasons in *Klayman*.[77] After Judge Leon issued his reasons in *Klayman*, an unknown party (presumably a telecommunications company) petitioned the FISC to "vacate, modify, or reaffirm" a s. 215 order. Judge Collyer of the FISC found Judge Leon's analysis in *Klayman* to be unpersuasive and concluded that it provided no basis for vacating or modifying the order in question. As did Judge Pauley in *Clapper*, Judge Collyer relied primarily on *Smith v. Maryland*, considering it to be the controlling case on the collection of telephony metadata.

Recent U.S. Supreme Court case law has cast some doubt on whether *Smith* continues to apply to all telecommunications metadata.[78] If *Smith* is no longer good law, much of the constitutional jurisprudence used to justify the s. 215 program will crumble away. Our view is that a search of a person's metadata is precisely what it appears to be: a highly intrusive government search into

---

[73] *Klayman* at 42
[74] 13 Civ. 3994 (WHP) (2013)
[75] 442 U.S. 735 (1979)
[76] *Clapper* at 44
[77] *In re Application of the FBI for an Order Requiring the Production of Tangible Things*, United States FISC, Docket No. BR 14-01
[78] See, for example, *Riley v. California*, 573 U.S. ____ (2014), discussed in M. Rotenberg and A. Butler, "Symposium: In *Riley v. California*, a unanimous Supreme Court sets out Fourth Amendment for digital age" (June 26, 2014) online: Scotusblog < http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/>.

the private lives of the citizenry, and this is true whether it is the Canadian or the United States doing the search.

The continued controversy over the United State's metadata program reveals the weakness of the Canadian government's argument that its own metadata program is in line with that of other nations. The fact that many western nations have experimented with programs that strip citizens of their privacy rights does not mean those programs are lawful, just, or effective. While the United States and other countries can provide important guidance on how our own domestic programs can be improved to better protect our civil liberties, these foreign programs must not be treated as the final word on the rights and liberties of Canadians. Given all that has transpired since September 11, 2011, we cannot take the policies of the United States as setting the standard of acceptability for Canada's own conduct. We can and must do better.

PART IV: CONCLUSION

About 20 years ago, in a case styled *Little Sisters Book and Art Emporium v. Canada,* I challenged the powers of Canada Customs to not only ban books at the border on the grounds that the books were obscene, but also to detain and inspect literally hundreds of thousands of books, magazines and videos on the basis that they might be obscene.[79] Out of the hundreds of thousands there was arguably the odd obscene book. Customs' argument for this sweeping power to detain and inspect was that unless they did so they wouldn't be able to catch that one evil book.

To some extent CSCE engages in this same dragnet approach to spying. We suspect that the Ministerial Authorizations used to intercept the private communications of Canada and CSEC's collection and analysis of metadata proceed on the premise that one cannot find the needle in the haystack unless one seizes and searches the haystack.

In my preparation for the *Little Sisters* case I was struck by the observation of Professor Thomas Emerson, one America's foremost First Amendment Scholars, who said this:

> A system of prior restraint normally brings within the complex of government machinery a far greater amount of communication than a system of subsequent punishment.[80]

Professor Emerson put it pithily when he said:

> The function of the censor is to censor. [...] The long history of prior restraint reveals over and over again that the personal and institutional forces inherent in the system nearly always end in stupid, unnecessary, and extreme suppression.[81]

I think those words apply to CSEC. The function of the spy is to spy, and the same forces that drive the censor also drive the spy: the boundless desire to over-collect and analyze what in the

[79] 2000 SCC 69
[80] T. Emerson, "The Doctrine of Prior Restraint" (`955), 20 Law and Contemporary Problems 648 at 656
[81] Emerson at 659

end is perfectly lawful, innocent and indeed constitutionally protected information and expression.

In the recent book *A Spy Among Friends,* which tells the gripping story of Britain's most infamous spy and double agent, Kim Philby, I was taken by the arrogance and sense of self-importance of those in Britain's MI6, one of whom described their role as follows:

> It is the spy who has been called upon to remedy the situation created by the deficiencies of ministers, diplomats, generals and priests [...] And so it is not surprising these days that the spy finds himself the main guardian of intellectual integrity.[82]

We are concerned that - like those in Britain's M16 - those in CSEC subscribe to this credo. They see themselves both as our protectors and as superior to the "ministers, diplomats, and generals", and no doubt and especially superior to our judges, who are properly tasked with protecting Canadians and advancing Canada's interest. Our objective in bringing this constitutional challenge is to see that the judiciary, who have long protected the rights of Canadians, are able to hold these "guardians" to the constitutional values they claim to protect. Only through judicial review can Canadians be confident that someone is indeed "watching the watchmen."

[82] B. Macintyre, *A Spy Among Friends: Kim Philby and the Great Betrayal* (New York: Crown Publishers, 2014)