LAW, LOGARITHMS AND LIBERTIES: LEGAL ISSUES ARISING FROM CSEC'S METADATA PROGRAM

Craig Forcese*

FIRST DRAFT – March 2014
Released on SSRN May 2014
Intended for University of Ottawa Press

Abstract

Two thousand and thirteen was the year of the spy. Edward Snowden – "leaker" or "whistleblower" depending on one's perspective – ignited a mainstream (and social) media frenzy in mid-2013 by sharing details of classified US National Security Agency (NSA) surveillance programs with the U.K. ***Guardian*** and ***Washington Post*** newspapers.

For related reasons, 2013 was also the year in which the expression "metadata" migrated from the lexicon of the technologically literate to the parlance of everyday commentary. The NSA revelations fuelled media, academic and other speculation about whether similar surveillance programs exist in Canada. That attention focused on Canada's NSA equivalent (and close alliance partner), the Communications Security Establishment Canada (CSEC). CSEC does have a metadata collection program, prompting questions about its legal basis, and the extent to which CSEC is governed by robust accountability mechanisms. This article focuses on a single aspect of this debate: By reason of technological change and capacity, have the state's surveillance activities now escaped governance by law? A broad question with a number of facets, this article examines the specific sub-issue of metadata and its relationship with conventional rules on searches and seizures. The article concludes that the privacy standards that CSEC must meet in relation to metadata are much more robust than the government seems to have accepted to date.

Table of Contents

* Vice Dean and Associate Professor, Common Law Section, Faculty of Law, University of Ottawa.

Introduction

Two thousand and thirteen was the year of the spy. Edward Snowden – "leaker" or "whistleblower" depending on one's perspective – ignited a mainstream (and social) media frenzy in mid-2013 by sharing details of classified US National Security Agency (NSA) surveillance programs with the U.K. ***Guardian*** and ***Washington Post*** newspapers.[1]

For related reasons, 2013 was also the year in which the expression "metadata" migrated from the lexicon of the technologically literate into the parlance of everyday commentary. The NSA, it would appear, collects and archives "metadata" on millions of internet and telecommunication users.[2] This information has been compared to "data on data" – that is, it the contextual information that surrounds the content of an internet transaction or communication. As described by the ***Guardian***, "[e]xamples include the date and time you called somebody or the location from which you last accessed your email. The data collected generally does not contain personal or content-specific details, but rather transactional information about the user, the device and activities taking place."[3]

---

[1] Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret programs," *Washington Post* (6 June 2013), <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html>; Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian* (6 June 2013) <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>.

[2] James Bell, "NSA stores metadata of millions of web users for up to a year, secret files show," *The Guardian* (30 Sept 2013) <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>; Greenwald, *supra* note 1.

[3] "A Guardian guide to your metadata," *The Guardian* (12 June 2013) <http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000>

The NSA revelations fuelled media, academic and other speculation about whether similar surveillance programs exist in Canada. That attention focused on Canada's NSA equivalent (and close alliance partner), the Communications Security Establishment Canada (CSEC). In 2013, journalists unearthed tantalizing clues concerning a Canadian metadata project.[4] In early 2014, a Snowden document pointed to some sort of CSEC metadata collection project implicating travellers accessing WiFi network at a Canadian airport.[5]

These disclosures prompted questions about the legal basis for any collection program, and the extent to which CSEC was governed by robust accountability mechanisms. They also sparked a constitutional lawsuit brought by the BC Civil Liberties Association.[6]

The Canadian government remained largely inert faced with these concerns, hewing to a policy of limited comment rather than more open debate.[7] The government's clear expectation has been that the controversies ignited by Snowden would eventually expire, if starved of oxygen. By the time of this writing, this hope appears not to have been realized. Mr. Snowden's chief journalistic partner, Glen Greenwald, has adopted a strategy of "serial" releases of Snowden documents, including a regular trickle of Canada-specific materials on various surveillance issues. This dribble of material – although single sourced, decontextualized and often difficult to understand -- has kept the matter in the public eye.

Meanwhile, CSEC and its partner CSIS have been caught in a seemingly unrelated surveillance controversy by exceeding the legal limits on surveillance imposed by Federal Court warrants.[8]

Together, these events have created more than the whiff of scandal surrounding Canada's surveillance activities. The undoubtedly unfair

---

[4] See, e.g., Colin Freeze, "How Canada's shadowy metadata-gathering program went awry," *Globe and Mail* (15 June 2013) < http://www.theglobeandmail.com/news/national/how-canadas-shadowy-metadata-gathering-program-went-awry/article12580225/?page=all#dashboard/follows/>

[5] Greg Weston, Glenn Greenwald and Ryan Gallagher, "CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents," CBC News (30 Jan 2014) <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881> . The actual CSEC document is posted at <http://www.cbc.ca/news2/pdf/airports_redacted.pdf>.

[6] See BCCLA, Notice of Civil Claim, Supreme Court of British Columbia < http://bccla.org/wp-content/uploads/2013/10/2013-10-22-Notice-of-Civil-Claim.pdf >

[7] See the CSEC responses to Snowden disclosures at <http://www.cse-cst.gc.ca/home-accueil/media/media-2014-01-30-eng.html> and < http://www.cse-cst.gc.ca/home-accueil/media/media-2014-01-29-eng.html>. See also the CSEC chief's testimony in front of the Standing Senate Committee on National Security and Defence, 41st Parl. 2nd Sess, Issue 2, Evidence (3 Feb 2014) <http://www.parl.gc.ca/content/sen/committee/412/SECD/02EV-51162-E.HTM>.

[8] *IN THE MATTER OF an application by [X] for a warrant pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act, R.S.C. 1985, c. C-23*, 2013 FC 1275.

impression left by the timing and frequency of these controversies is of recidivist skullduggery by the Canadian spy services.

The purpose of this article is not, however, to rehearse these events or assess the merits or demerits of Canada's national security surveillance actions. Instead, I focus on a narrower, but in my view, even more fundamental question: By reason of technological change and capacity, have the state's surveillance activities now escaped governance by law? A broad question with a number of facets, this article examines the specific sub-issue of metadata and its relationship with conventional rules on searches and seizures.

I proceed in two main parts. In part I, I trace what is currently known about CSEC's metadata activities. In part II, I examine two specific legal questions raised by these activities: first, the extent to which metadata are "private communications" that attract certain statutory privacy protections; and, second, whether CSEC metadata collection is consistent with section 8 of the ***Canadian Charter of Rights and Freedoms***.[9] The discussion in this article is provisional, by dint of imperfect information about CSEC activities. Based on what we do know, however, I argue that the privacy standards that CSEC must meet in relation to metadata are much more robust than the government seems to have accepted to date.

Part I: Canada's Metadata Surveillance Programs

It is, of course, impossible to outline in anything close to full form CSEC's metadata collection program. Nevertheless, enough in now on the public record that something may be said about it.

It is important, however, to begin with a brief discussion of metadata and its implications for privacy. I then turn to a review of CSEC and its functions, so that readers may contextualize the more specific information on metadata collection. Finally, this section traces what is known about CSEC's metadata operations.

A. Metadata in Context

In this initial section, I discuss the nature and privacy implications of "metadata".

In a 2013 report, the Privacy Commissioner of Ontario defined "metadata" as "information generated by our communications devices and our communications service providers, as we use technologies like landline telephones, mobile phones, desktop computers, laptops, tablets or other computing devices. It is essentially information about other information, in

---

[9] Part I, *The Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.

this case, relating to our communications."[10] The Commissioner compared metadata to "digital crumbs" that reveal "time and duration of a communication, the particular devices, addresses, or numbers contacted, which kinds of communications services we use, and at what geolocations."[11]

This information is stored by communications providers for differing periods of times, and is amendable to compilation, linking and tracing. Metadata can be used to paint a quite intimate portrait: work and sleep habits, travel patterns, and relationships with others. From these data, observers may develop detailed inferences about places of employment, patterns and means of travel, frequency of visits to doctors and pharmacies, visits to "social or commercial establishments", religious and political affiliations and the like.[12]

Reviewing this kind of information may be more invasive of privacy than even intercepting the actual content of communications. MIT computer scientist Daniel Weitzner considers metadata "arguably more revealing [than content] because it's actually much easier to analyze the patterns in a large universe of metadata and correlate them with real-world events than it is to through a semantic analysis of all of someone's email and all of someone's telephone calls…".[13]

Metadata associated with internet use may also reveal notable amounts of personal information. A study by the Privacy Commissioner of Canada concluded that subscriber information such as IP addresses[14] may "provide a starting point to compile a picture of an individual's online activities, including: online services for which an individual has registered; personal interests, based on websites visited; and organizational affiliations."[15]

Even more concerning than the direct privacy implications of metadata is the amalgamation of these data with other information, a process that some have called "Big Data". A colloquial expression, one definition of "Big Data is "the storage and analysis of large and/or complex

---

10 Ann Cavoukian, *A Primer on Metadata: Separating Fact from Fiction* (Information an Privacy Commissioner, Ontario, July 2013) at 3.

11 *Ibid*.

12 *Ibid* at 4.

13 E. Nakashima, "Metadata reveals the secrets of social position, company hierarchy, terrorist cells," *Washington Post* (15 June 2013), cited in Cavoukian, *supra* note 10 at 3.

14 An IP address "is a numerical identification and logical address that is assigned to devices participating in a computer network utilizing the Internet Protocol." Office of the Privacy Commissioner of Canada, *What an IP Address Can Reveal About You* (May 2013) <http://www.priv.gc.ca/information/research-recherche/2013/ip_201305_e.asp>.

15 *Ibid*.

data sets using a series of [computer-based] techniques."[16] Big Data may involve the linking of discrete and separate pieces of information together to create a "mosaic" portrait of a person's life.

B. An Overview of CSEC's Mandates

By law, CSEC's mandate includes: acquiring and using "information from the global information infrastructure for the purpose of providing foreign intelligence" ("Mandate A") and providing "technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties" ("Mandate C").[17] In other words, it is principally an electronic eavesdropping agency that collects what is known as "signals intelligence", SIGINT.

However, in order to perform any spying, CSEC must be lawfully authorized to do so – that is, it must be able to lawfully access the electronic data. CSEC may spy on foreigners and on Canadians, but the rules that apply to each of these scenarios are radically different.

1. Mandate A and Lawful Access

First, under its Mandate A, CSEC can collect "foreign intelligence" – that is, "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".[18] Much (probably almost all) of this foreign intelligence is just that: foreign. There is no Canadian or person in Canada implicated in the intercepted communication. Here, the law does not prescribe any specific rules on intercept authorizations.

On the other hand, CSEC's rules insist that its foreign intelligence activities "not be directed at Canadians or any person in Canada; and ... shall be subject to measures to protect the privacy of Canadian in the use and retention of intercepted information."[19]

Squaring this expectation with the reality of webbed communication is challenging. In a world whose telecommunications systems are webbed together, even "foreign intelligence" may have a Canadian nexus – for instance, it may be that a telephone call sent to or originating in Canada

---

16 "The Big Data Conundrum: How to Define It?" *MIT Technology Review* (3 Oct 2013) <http://www.technologyreview.com/view/519851/the-big-data-conundrum-how-to-define-it/>.

17 *National Defence Act* (*NDA*), R.S.C., 1985 c. N-5, s. 273.64. CSEC also provides "advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada". This Mandate "B" does not, however, figure in this article.

18 *Ibid*, s. 273.61.

19 *Ibid*, s. 273.64.

might be intercepted. Similarly, CSEC surveillance may capture the communication of a Canadian located overseas. As the government acknowledges, "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."[20]

CSEC's law recognizes that "there may be circumstances in which incidental interception of private communications or information about Canadians will occur."[21] The law permits the Minister of National Defence to issue a "ministerial authorization" authorizing CSEC to collect "private communications". The minister may issue this authorization only where satisfied, among other things, that the interception is directed at foreign entities outside of Canada and privacy-protecting measures are in place in the event that Canadian communications are captured. [22]

"Private communication" in CSEC's law is defined with reference to Part VI of the ***Criminal Code***, described further below.[23] Part VI makes it a crime to intercept a "private communication" in most instances, when done without authorization. Under its law, the ministerial authorization exempts CSEC from this criminal culpability.[24] The authorization presumably also makes an intercept "lawfully made", and excuses the government from the civil liability that otherwise exists for intercepting "private communications".[25]

Under these circumstances, it is obviously critical that the government agency have a clear-eyed view of what constitutes "private communication" and that it act assiduously in obtaining the required authorization for its intercept.

In practice, ministerial authorizations have been issued on a "just in case" basis – that is, because one can never be sure that the communications intercepted will lack a Canadian nexus, authorizations are sought regularly to make sure CSEC remains on-side the law. Compared to warrants issued by judges in police investigations (and those by the Canadian Security Intelligence Service), ministerial authorizations are general. As described by the commissioner charged with review of CSEC in

---

20 Government of Canada, Attorney General of Canada, *Response to Civil Claim*, in BC Civil Liberties Association v. AG of Canada, Supreme Court of British Columbia, No. S137827, 20 Jan 2014, at para. 5, on file with author (hereafter "GOC Response").

21 *Ibid* at para. 5.

22 NDA, *supra* note 17, s.273.65(1).

23 *Criminal Code*, R.S.C., 1985, c. C-46.

24 NDA, *supra* note 17, s. 273.69 ("Part VI of the *Criminal Code* does not apply in relation to an interception of a communication under the authority of an [ministerial] authorization issued under this Part or in relation to a communication so intercepted")

25 *Crown Liability and Proceedings Act*, R.S.C. 1985, c. C-50, s. 17.

his 2011-12 annual report, ministerial authorizations "relate to an 'activity' or 'class of activities' specified in the authorizations ... the authorizations do not relate to a specific individual or subject (the whom or the what)."[26]

The minister issued a total of 78 authorizations between 2002-2012.[27] For 2011, six authorizations existed, and CSEC intercepted private communication in relation to only one of these authorizations.[28]

2. Mandate C and Lawful Access

In addition, CSEC may also assist CSIS or the RCMP in intercepting information, providing technological wherewithal that other agencies may not have. Given the mandate of the latter bodies, these intercepts would usually involve Canadians or communications within Canada. Such domestic intercepts would only be legal if CSIS or RCMP themselves had lawful authority for the intercept.

In practice, that legal authority depends on a judge pre-authorizing the intercept by judicial warrant or authorization. CSEC, in other words, would only spy on Canadians on behalf of CSIS or the RCMP where these agencies themselves were lawfully permitted to perform the surveillance.[29] The legal authority exercised by the requesting agency creates a safe harbour for CSEC.

C. Metadata Collection by CSEC

I turn now to a description of CSEC's metadata collection programs under its Mandate A. This assessment relies on often deeply redacted documents obtained mostly by ***Globe and Mail*** journalist Colin Freeze, under the ***Access to Information Act***.

1. 2004 to 2008

On March 14 2004, the Minister of National Defence issued a "ministerial directive" to CSEC, pursuant to his power to do so under the ***National Defence Act***.[30] While the full title of this directive is redacted from

---

[26] Commissioner of the Communications Security Establishment, *2011-2012 Annual Report* < http://www.ocsec-bccst.gc.ca/ann-rpt/2011-2012/5_e.php>. See also GOC Response, *supra* note 20 at paras 7 and 8.

[27] *Ibid* at para 14. These presumably included authorizations under CSEC's IT security mandate (Mandate B), not discussed in this article.

[28] *Ibid* at para 16.

[29] NDA, *supra* note 17, s.273.64(3).

[30] Hereafter, March 2004 Ministerial Directive (on file with the author). Except as otherwise noted, all documents referred to in this section were obtained by Colin Freeze of the Globe and Mail under access to information law. As described by the government, "Ministerial directives do not grant any authority that does not already exist in law and cannot enhance any existing authority.

documents released under the access law, it clearly concerned (at least in part) collection by CSEC of telecommunications metadata under that agency's Mandate A.

The public document is deeply censored and details on the program (including the definition of "metadata") are deleted. The directive does, however, specify that CSEC "will not direct program activities at Canadians or at any person in Canada." It also obliged the agency to apply its existing privacy protection procedures on "use and retention of communications and data". CSEC could share metadata with other agencies, but "subject to strict conditions to protect the privacy of Canadians, consistent with the standards governing CSE[C]'s other programs".

The Minister replaced this initial instrument with another directive, dated March 9, 2005 and entitled "Ministerial Directive, Communications Security Establishment Collection and Use of Metadata".[31] The public version of document again excises a full definition of "metadata", but states that "metadata" "means information associated with a telecommunication to identify, describe, manage or route that telecommunications or any part of it".

Again, the Ministerial Directive tasked CSEC with metadata collection under its foreign intelligence mandate (Mandate A),[32] and repeated language on compliance with existing privacy protections. These privacy strictures were apparently enumerated in detail, but the actual protections are redacted from the document. The directive also acknowledges the responsibility of CSEC's review body, the Commissioner of the CSEC. CSEC's law charges this Commissioner with, among other things, reviewing "the activities of the Establishment to ensure that they are in compliance with the law".[33]

The Commissioner undertook such a review, dated January 2008, in order to "identify and understand the nature of CSE[C]'s metadata activities and to assess their compliance with the ministerial directive and with the laws of Canada" and CSEC's "own operational policies, procedures and practices".[34] Much of the Commissioner's report is redacted. It is clear, however, that legal advice provided by the Department of Justice undergirded CSEC's metadata collection process. For reasons excised from

---

They serve as additional direction or guidance, setting out the Minister's expectations for, or imposing restrictions on, CSE. Where a Ministerial directive applies, CSE's activities must be consistent with that Ministerial directive." GOC Response, above note 20 at para 17.

31 Hereafter, March 2005 Ministerial Direction (on file with the author).

32 The directive also points to CSEC's mandate to protect government cyber systems, a Mandate B issue not discussed further in this article.

33 NDA, *supra* note 17, s.273.63(2).

34 OCSEC Review of the Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata, March 9, 2005 at 2 (on file with author).

the public document, the Commissioner concluded that at least some metadata collection activities under the directive did not require ministerial authorization,[35] presumably because they did not implicate "private communications".

However, there are other passages in the Commissioner's report suggesting that some metadata was collected pursuant to a ministerial authorization, "as it is possible that a private communication could be intercepted".[36] Indeed, the Commissioner recommended that CSEC "re-examine and re-assess its current position and practice that requires that only those private communications recognized [redaction] be accounted for."[37]

2. 2008 to Present

The Commissioner's report and other Commissioner documents also raised doubts as to whether CSEC acted properly in conducting metadata collection under its Mandate A that should, in fact, have been sought under Mandate C, assistance to security and law enforcement agencies. In his report, the Commissioner asks: "[i]s CSE[C]'s (a) mandate the appropriate authority to conduct [redaction] in the context of a criminal or national security investigation of a Canadian in Canada?"[38] The Commissioner ultimately called on CSEC to re-examine and reassess the legislative authority used to conduct at least some of its (presumably) metadata activities.[39]

The position was contested by CSEC, apparently on the strength of legal advice obtained from the Department of Justice.[40] However, in a follow-up letter to the Minister of National Defence, the Commissioner noted his view that the issue was not the interpretation of Mandates A and C, but which mandates applied in which context. He underscored the significance of the distinction between Mandate A and C: deciding which applies "is important because [among other things] it determines the legal requirement (e.g. ministerial authorization vs a court warrant) in cases where activities may be 'directed at' a Canadian…".[41]

---

35 *Ibid* at 7.

36 *Ibid* at 16.

37 *Ibid* at 32.

38 *Ibid* at 18. See also pages 22 – 24, raising the same doubts and suggesting that some metadata activities were properly something that should have been pursued under Mandate C.

39 *Ibid* at 24.

40 Letter to Minister MacKay from CSEC Chief John Adams (undated) (on file with author).

41 Letter to Minister MacKay from Commissioner Gonthier (16 Sept 2008) (on file with author).

Despite these differences of opinion, the Commissioner's concerns were apparently enough to prompt CSEC to suspend its metadata program during the period April 2007 to October 2008. CSEC recommenced the project thereafter, but apparently with changes. According to ministerial media lines, the initial suspension "was initiated by the Chief of CSEC, in order to make absolutely certain that the activities in question were compliant with Canadian privacy laws as well as with CSEC's own policies and procedures. … In consultation with the Department of Justice an internal review determined that these activities were indeed in compliance with the law but I felt that certain CSEC policies should be clarified. This was done and CSEC resumed these activities."[42]

A December 2010 report by the CSEC Commissioner examined CSEC's re-commenced metadata activities from October 2008-October 2009. According to a 2011 CSEC briefing note, that report concluded that activities "were appropriately authorized under part (a) of the mandate," and the Commissioner no longer had concerns as to whether activities should instead be conducted under Mandate C.[43]

The 2005 ministerial directive itself changed in late 2011.[44] According to briefing notes prepared in support of 2011 change, CSEC concluded that something redacted (but in context, perhaps metadata) "does not represent a reasonable threshold for privacy concerns and therefore current privacy protection measures are adequate".[45] It is also clear that "metadata" were not, in CSEC's view, "a communication".[46] Indeed, in its Ops-Manual, CSEC writes that "metadata" "does not required an MA [ministerial authorization]",[47] something that could only be true if CSEC viewed metadata as outside the scope of private communication. These conclusions are relevant to the legal analysis that follows in Part II of this article.

---

42 Advice to the Minister, CSEC Issues (19 Dec 2011) (on file with author) <http://www.theglobeandmail.com/news/national/raw-documents-canadas-top-secret-data-mining-program/article12446852/?from=12444909#dashboard/follows/

43 Scenario Note for Chief's Briefing to the National Security Advisor (10 Jan 2011) (on file with the author).

44 Ministerial Directive, Communications Security Establishment, Collection and Use of Metadata (21 Nov 2011) (on file with author) < http://www.theglobeandmail.com/news/national/raw-documents-canadas-top-secret-data-mining-program/article12446852/?from=12444909#dashboard/follows/

45 Memorandum for the Chief: Updated Collection and Use of Metadata Ministerial Directive (14 Nov 2011) at 18 (in file) and 14 (on document) (on file with the author <http://www.theglobeandmail.com/news/national/raw-documents-canadas-top-secret-data-mining-program/article12446852/?from=12444909#dashboard/follows/>

46 *Ibid* at 20 (in file).

47 CSEC, OPS-1 *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities* (Effective date: 1 Dec 2012) at 5 (on file with the author).

The government's position on some privacy questions may since have shifted, at least in a small way. In February 2014, it specified that "metadata" means "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information or part of information which could reveal the purport of a telecommunication, or the whole or part of its content".[48] It seems also to acknowledge that collection of at least some metadata may give rise to a reasonable expectation of privacy, although interference with this expectation is reasonable because, among other things, of ministerial authorizations.[49]

Part II: Metadata and the Law

I turn now to legal issues raised by the metadata program described in Part I. To encapsulate the apparent government position suggested by the documents described above: the government may not regard "metadata" as constituting a "private communication". Exactly why this is so is unknown, but may reflect the government view that metadata are ***per se*** not communication. While its position may be shifting, it may also not view metadata as giving rise to a "reasonable expectation of privacy" or their collection as constituting an unreasonable search and seizure.

These findings are crucial. If metadata are private communications, then their collection must be supported by a ministerial authorization in order to be exempted from application of the criminal law (and civil liability exposure). If any of CSEC's activities (with metadata or elsewhere) give rise to a reasonable expectation of privacy, section 8 Charter issues arise, with serious implications not only for the collection process but also more generally for the constitutionality of CSEC's ministerial authorization regime.[50]

A. Metadata May Be "Private Communication"

In both CSEC's law and Part VI of the ***Criminal Code***, "private communication" means

---

48 GOC Response, above note 20 at para 1.

49 *Ibid*, Div 3, paras. 6-7. See discussion part II below.

50 A third issue relates to the question of *vires*; that is, whether CSEC collects metadata pursuant to the correct mandate in its statute. This matter has obviously been the source of considerable discussion inside of government, and is not a question that can be plumbed in greater depth here, given the paucity of public documents that contextualize the debate. For the balance of this article, I assume that metadata is collected correctly under a Mandate A justification – that is, it relates to foreign intelligence and not assistance to law enforcement or CSIS. I do not address in this article a related issue: the precise sweep and contours of Mandate A.

> any ***oral communication***, or any ***telecommunication***, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is 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 person intended by the originator to receive it…[51]

This definition may be apportioned into key constituent elements. First, the provision pertains to a communication – whether "oral" or a "telecommunication". Second, the "originator" must have an expectation that the communication is, in fact, private – that is, that it will not be shared with a third party intermediary. In this respect, the courts have sometimes spoken about a reasonable expectation of privacy,[52] creating a link of sorts between "private communication" and the threshold for Charter section 8 protections. Third, the communication must be in Canada, or the communication must be intentionally directed at a person who is in Canada.

I discuss each of these elements in turn.

1. Metadata Falls within the Meaning of "Telecommunication"

Enacted in 1974, Part VI pre-dates modern communications technologies. The concept of "private communications" has, however, been the subject of judicial construals over the decades, as technology changes.

Private communication includes a "telecommunication", a concept that most people once would have associated with voice communication over telephone wires. However, the federal ***Interpretation Act*** prescribes a broader understanding, defining "telecommunication" as "the emission, transmission or reception of signs, signals, writing, images, sounds or intelligence of any nature by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system".[53]

In ***R. v. Telus Communications***,[54] a plurality of the Supreme Court of Canada relied on the ***Interpretation Act*** to conclude that "text messages" – that is, a written form of electronic communication – were clearly a "telecommunication" for the purposes of Part VI of the Criminal Code. Lower courts have reached similar conclusions. In ***R. v. Mills***, the

---

51 *Criminal Code*, *supra* note 23, s.183.

52 See, e.g., *R. v. Telus*, 2013 SCC 16, at para. 26 (per Abella J)

53 *Interpretation Act*, R.S.C., c. I-21, s. 35.

54 *Telus*, *supra* note 52 at para. 26.

Newfoundland and Labrador Provincial Court held that "private communication" included "emails and chat messages".[55]

These cases concerned intercept of content-rich data – actual communications. However, in ***Telus***, the plurality saw Part VI's rules on intercept of private communication as reaching the "state acquisition of informational content – the substance, meaning, or purport – of the private communication. ***It is not just the communication itself that is protected, but any derivative of that communication that would convey its substance or meaning***."[56] Likewise, in ***Lyons***, the Court concluded that Part VI was not "'wiretapping' legislation, nor eavesdropping legislation, nor radio regulation. It is the regulation of all these things and 'any other device' that may be used to intercept intelligence reasonably expected by the originator not to be intercepted by anyone other than the intended recipient."[57]

As suggested in Part I, metadata meets these thresholds precisely; it is derivate of the communication, but from it much substance can be inferred. It communicates, in other words, "intelligence", something the ***Interpretation Act*** makes part of "telecommunication". Indeed, "intelligence" is exactly why the security services seek to collect it.

The Supreme Court has also signaled its concerns with metadata in other contexts, other than Part VI. It has noted that the accumulation of metadata on computer systems is one reason why privacy protections on computer searches should be robust. In the Court's words:

---

55 [2013] N.J. No. 395 at para. 22. That court seems to have in part been motivated by the immediacy of the exchanges between the participants. This immediacy concept reflects, in part, the notion that Part VI only applies to an "intercept". In Part VI "intercept" "includes listen to, record or acquire a communication or acquire the substance, meaning or purport thereof." Some courts have held that an "intercept" must be contemporaneous with the communication. Part VI does not apply, in other words, to search of stored communications. *R. v. Bahr*, 2006 ABPC 360 at para. 42; *R. v. Singh*, 2012 ONSC 3633. This approach was rejected by Abella J, for a plurality of the Supreme Court in *Telus*, *supra* note 52: "A technical approach to 'intercept' would essentially render Part VI irrelevant to the protection of the right to privacy in new, electronic and text-based communications technologies, which generate and store copies of private communications as part of the transmission process … A narrow or technical definition of 'intercept' that requires the act of interception to occur simultaneously with the making of the communication itself is therefore unhelpful in addressing new, text-based electronic communications. " Abella J., for a plurality, at paras 33 and 34. (The Abella position was been followed in *R. v. Croft*, 2013 ABQB 640.) For his part, Moldaver J, writing for himself and another, appears also to accept that the recording of a communication by the telecommunications company does not exonerate the police from obtaining a Part VI authorization. Moldaver J. at para. 67 et seq. As Moldaver J. correctly notes, it would artificial and unrealistic to distinguish (for the purposes of Part VI) privacy protection between a communication captured instantaneously and one captured on a time delay, however short or long.

56 *Telus*, *supra* note 52 (per Abella) at para. 25 (emphasis added).

57 *Lyons v. The Queen*, [1984] 2 S.C.R. 633 at 664.

> Word-processing programs will often automatically generate temporary files that permit analysts to reconstruct the development of a file and access information about who created and worked on it. Similarly, most browsers used to surf the Internet are programmed to automatically retain information about the websites the user has visited in recent weeks and the search terms that were employed to access those websites. Ordinarily, this information can help a user retrace his or her cybernetic steps. In the context of a criminal investigation, however, it can also enable investigators to access intimate details about a user's interests, habits, and identity, drawing on a record that the user created unwittingly…[58]

All of this is to say that metadata constitute revealing, personal information from which potentially intimate content data can be inferred. There is good reason, therefore, to posit the inclusion of metadata as "telecommunication", and therefore as "private communication".

2. Precedent Tends to Support Metadata's Inclusion in "Telecommunication"

This conclusion is bolstered, to a point, by caselaw dealing with close analogues to metadata: information collected by telephone number recorders (TNRs). TNRs record the "telephone number or location of the telephone from which a telephone call originates, or at which it is received or is intended to be received".[59] Collection of this information is now regulated by a separate ***Criminal Code*** provision.[60] Both before and after the introduction of this provision, however, cases considered the applicability of Part VI to TNR information. These cases fall into three camps.

First, a minority of cases concludes that the data recorded by TNRs are not captured by the definition of "private communication" because Part VI only protects content-rich communications. In the eyes of these judges, private communication involves the exchange of information between

---

58 *R v. Vu*, 2013 SCC 60 at para. 42.

59 *Criminal Code*, *supra* note 23, s.492.2(4).

60 *Ibid*.

originator and recipient not the "the fact that a means of communication has been engaged".[61]

These decisions are difficult to reconcile with the concept of "telecommunications" noted above, and indeed tend to disregard the ***Interpretation Act***.[62] Not surprisingly, therefore, a second set of cases has viewed TNR data as "private communication",[63] plain and simple. Yet a third, more recent category of cases has agreed that data created by these devices are "telecommunications" under Part VI, but that the concept of "private communication" has no bearing where the communicator "knows some or all of it will or might be collected by the phone company in the normal course of business".[64] Put another way, the fact that the data is obtained by the authorities from a third party intermediary changes its character to something other than a "private communication".

3. Collection from Third Party Intermediaries Does Not Always Remove Metadata from the Class of "Private Communications"

The metadata collected by CSEC may often be obtained from third party communication service providers. It is important, therefore, to examine closely the question of "third party intermediaries" and its relevance to the concept of "private communications".

In this regard, I believe there is reason to doubt whether the view expressed by this third class of cases in relation to TNR data applies to the broader range of metadata telecommunications.

a) Past Cases on this Issue Have Been About Which Privacy Regime Applies, Not About Negating the Application of Any Privacy Regime

First, it is important to underscore that Parliament has now created a separate warrant regime for telephone number recorders. The recent cases that have excluded TNR data from "private communication" have not, therefore, had to decide between "privacy protection or no privacy

---

61 *R. v. Fegan* (1993), 80 C.C.C. (3d) 356 (On CA) at p.366. See also *R. v. Beck*, [1993] B.C.J. No. 1141 (QL); *R. v. Samson* (1983), 45 Nfld. & P.E.I.R. 32 (Nfld. C.A.).

62 In *R. v. Skrepetz,* [1990 BCJ No. 1467 (BC Prov Ct), the Crown even argued that recourse to the *Interpretation Act* was improper and inconsistent with the Supreme Court's approach. This position, even if correct at the time, has obviously been completely superseded by *Telus*, *supra* note 52.

63 See, e.g., *R. v. Griffith* (1988), 44 C.C.C. (3d) 63 (Ont. Dist. Ct.); *R. v. Khiamal* (1990), 73 Alta. L.R. (2d) 359 (Q.B.); *R. v. Mikituk* (1993), 101 Sask R. 286 (Q.B.)

64 *R. v. Lee*, 2007 ABQB 767 at para. 282. See also *Croft*, *supra* note 55 at para. 22 (following *Lee* on this issue).

protection". Instead, they have dealt with the issue in the context of "***which*** privacy protection".

In ***Lee***, for example, the Alberta trial court concluded that Part VI was inapplicable because of the third party intermediary, but emphasized that this "is not to say the originator does not have some expectation of privacy in the TNR data". In fact, Parliament had enacted special provisions on TNR that "may be taken to reflect Parliament's recognition there is a reasonable expectation of privacy in TNR data, albeit a somewhat diminished expectation." The court then observed that the "TNR device nowadays may well capture more than telephone numbers, date and time of telephone contact and nearest cellular telephone tower. It may also record passwords, pin numbers, or other number-based codes keyed in using the number pad on the telephone. The very fact contact was made between certain telephone numbers may reveal some aspects of lifestyle."[65]

The existence of a transparent, TNR-specific judicial authorization regime places that issue on a dramatically different footing than the subject of this article: intercept of potentially even more revealing metadata by CSEC ***without*** any third party authorization ***whatsoever***. If an intercept is not private communication, CSEC may act without any advance, third party scrutiny. Since this is fully lawful, the Commissioner's review will not detect any defect in this behaviour. Put another way, defining metadata as outside the ambit of "private communication" would give exclusive intercept authority to an intelligence service whose conduct will never come to light or be second-guessed, except through happenstance.

I hypothesis, therefore that a court would be much more reluctant to define metadata as falling outside the ambit of "private communication" when the result is a ***carte blanche*** for an intelligence service. By way of rough analogy, the Supreme Court has condemned past construal of the law that "by-passes any judicial consideration of the entire police procedures and thereby makes irrelevant the entire scheme in Part IV.1 of the Code".[66]

All of this is to say that the third class of TNR court decisions is distinguishable from the subject matter of this article.

b) The Reasonable Originator Would Not be Aware of the Full Scope of Third Party Access to Metadata

Second, it is clear that under the definition of "private communication," "[i]t is the originator [of the communication's] state of mind that is

---

65 *Lee*, *supra* note 64, at para. 283.

66 *R. v. Duarte*, [1990] 1 SCR 30 at para. 47.

decisive."[67] Put another way, the "private" nature of the communication turns on whether the "sender of such communications can reasonably expect that they will not be intercepted by any person other than the persons intended to receive them"[68] The existence of a third party intermediary goes to the reasonableness of the originator's expectation of privacy.

This is exactly the issue raised by the third class of TNR cases. A reasonable originator should properly realize that TNR data in the possession of service providers is not confidential information – not least, it is used for billing purposes. However, what an originator should believe about a telephone's company's access to TNR data is quite different than what he or she should reasonably believe about other, more arcane forms of metadata.

It is not clear as a factual matter that a reasonable observer would, or should, appreciate the full extent of the metadata attached to a modern communication, undertaken with different devices. Nor does it seem plausible, as communications technologies proliferate and converge, that a reasonable originator should be expected to appreciate the precise degree to which a third party intermediary may be privy to this metadata.

For instance, would a reasonable observer be able to distinguish between conventional telephone calls, voice calls made over a cell service, voice calls make over an VoIP system, and voice calls made over a peer-to-peer service such as Skype? These different technologies may produce different sorts of metadata, and there may be differences in the extent to which a third party intermediary may record and have access to this data. Moreover, service providers (an increasingly varied and international class) may differ in the extent to which they collect and archive this information, or adhere to whatever policies they do have. As an empirical matter, the "reasonable originator" probably lacks the technological literacy to really understand what is and can be collected about his or her communication by a third party intermediary.

Of course, in the wake of the Snowden revelations, that reasonable originator might now be adjudged a paranoid originator. Faced with revelations about the scope of government intercepts and the extent to which communication companies do (or are compelled to) cooperate, an argument might be made that no reasonable originator should assume privacy in ***any*** of their telecommunication.

Put another way, the invasiveness of government surveillance and the evolution of the technology that allows this surveillance has the effect of

---

67 *R. v. Goldman*, (1979), 13 C.R. (3d) 228 at 248 et seq. (S.C.C.). Note that the Supreme Court did not equate "originator" with "person who made the call". Rather, the originator is the person who made the statement/communication that the police now wish to use.

68 *Ibid*.

redefining the expectations of the reasonable person. If these developments (and whatever notoriety is attached to them) are in turn used to determine the scope of the reasonable person's expectations, the result is a vicious spiral that further and further erodes the scope of "private communications". The end result is that the concept of "private communication" is rendered moot, something that would make a mockery of Parliament's obvious intent to protect the integrity of telecommunication privacy.

It would also run counter the position articulated by the Supreme Court in its ***Charter*** section 8 jurisprudence. There, the Court has rejected the idea that "as technology developed, the sphere of protection for private life must shrink".[69] In a ***Charter*** section 8 case involving an intercepted conversation with an informer, the Court held:

> No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being. On the other hand, the question whether we should countenance participant surveillance has everything to do with the need to strike a fair balance between the right of the state to intrude on the private lives of its citizens and the right of those citizens to be left alone.[70]

Neither paranoia nor ubiquitous state surveillance set the standard for the reasonable person.[71] The reasonable expectation of privacy is a normative concept that does not vary with naiveté and the risk that people's privacy expectations may be dashed. As the Supreme Court observed in yet another section 8 case, "[i]n an age of expanding means for snooping readily available on the retail market, ordinary people may come to fear (with or without justification) that their telephones are wiretapped or their private correspondence is being read … Suggestions that a diminished ***subjective*** expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed."[72]

It stands to reason that a similar logic applies to Part VI and "private communication".

---

69 *R. v. Tessling*, 2004 SCC 67 at para 16.

70 *Duarte*, *supra* note 66 at para 32.

71 See *R. v. Ward*, 2012 ONCA 660 at para 87, and cases there cited.

72 *Tessling, supra* note 69 at para 42.

c) The Explosion of Data in the Hands of Third Parties Should Not Undermine Privacy Protections

Third, a plurality of the Supreme Court in ***Telus*** resists using the modern ubiquity and permanence of data in hands of third party service providers to undermine the scope of privacy protections in Part VI. There, it emphasized that "[t]he communication process used by a third-party service provider should not defeat Parliament's intended protection for private communications. … [T]his Court has recognized in other contexts that telecommunications service providers act merely as a third-party 'conduit' for the transmission of private communications and ought to be able to provide services without having a legal effect on the nature (or, in this case, the protection) of these communications."[73]

As noted, the case concerned intercept of text messages. While the issue was not before the Court, there is no principled basis to treat telecommunications in the form of text or content data differently from telecommunications that comes in the form of metadata surrounding that content. If the third party intermediary rule does not apply to one form of telecommunications, it should not apply to the other.

In sum, there are very compelling reasons to conclude that at least some metadata created through communications over a third party conduit remain "private communication".

4. Metadata May Meet the Geographic Requirements of "Private Communication"

Geography is a final consideration raised by definition of "private communication". A "private communication" is "one made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada". It follows that only those communications that have a beginning and end outside of the territory of Canada are excluded from "private communication".

Notably, the government may not "outsource" collection of a private communication to a foreign allied agency to circumvent the rules on "private communication". As the Federal Court has observed, "Canadian law cannot either authorize or prohibit the second parties [i.e., the foreign allies] from carrying out any investigation they choose to initiate with respect to Canadian subjects outside of Canada. That does not exempt

---

[73] *Telus*, *supra* note 52 at para 41 per Abella J (for a plurality).

Canadian officials from potential liability for requesting the interception and receiving the intercepted communication."[74]

5. Conclusion

In sum, if CSEC acts on legal advice that denies metadata "private communication" status, it does so at considerable risk. The matter has not yet been decided definitively. However, it is now more reasonable to assert that metadata ***are*** "private communication" than to assert that they are not. Because an incorrect conclusion about metadata's status as "private communication" opens the door to criminal culpability and civil liability for its unauthorized intercept, the government would be prudent to seek full "private communication" authorization for metadata collection activities having a possible Canadian geographic nexus.

B. Metadata and the Charter

"Private communications" under Part VI of the Criminal Code is data in relation to which a person has a reasonable expectation of privacy, and to which Charter section 8 protections also apply.

But while all "private communications" may be protected by section 8, it does not follow that section 8 is limited to "private communications". This is a banal statement, since the ***Criminal Code*** is replete with other warrant requirements above and beyond Part VI designed to meet section 8 standards in relation to other forms of search and seizure.

This section considers, therefore, whether metadata are protected by section 8, regardless of how they might be treated by courts for purposes of Part VI and its concept of "private communication".

I begin with a brief overview of section 8 and its rules. I then apply those rules to the CSEC metadata program.

1. Basics of Section 8

Section 8 guarantees the right to be free from unreasonable searches and seizures.[75] In practice, the section 8 analysis turns on "whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement."[76]

---

74 *In the MATTER OF an application for a warrant pursuant to Sections 12 and 21 of the Canadian Security Intelligence Service Act*, 2013 FC 1275 at para. 101.

75 *Constitution Act* 1982, *supra* note 9. See *Lavigne v. Canada (Commissioner of Official Languages),* [2002] 2 S.C.R. 773 at para. 25 (labelling this a privacy right).

76 *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145 at 159–60.

In consequence, a section 8 analysis raises two questions: first, has there been a search or seizure; second, if so, was that search or seizure reasonable.[77]

a) Reasonable Expectation of Privacy

A search or seizure is equated, in practice, with the existence of a "reasonable expectation of privacy"[78], one that includes both a subjective and objective expectation.[79] The Supreme Court has spoken of three "zones" of privacy: "The territorial zone refers to places such as one's home. Personal or corporeal privacy is concerned with the human body (body, images such as photographs, voice or name)." Finally, a person has a right to informational privacy, or "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others".[80] Information attracting constitutional protection includes "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[81]

Electronic surveillance may transgress a reasonable expectation of privacy and constitute a search and seizure regulated by section 8 of the ***Charter***.[82] The Supreme Court has described its jurisprudence in this area as "embrac[ing] all existing means by which the agencies of the state can electronically intrude on the privacy of the individual, and any means which technology places at the disposal of law enforcement authorities in the future."[83]

However, whether a particular electronic intercept activity amounts to a "search" remains highly fact specific. In defining the scope of this "reasonable expectation" in individual instances, Canadian courts have focused on the "totality of circumstances"[84] and have spoken of the privacy expectation being "normative" and not "descriptive."[85] That is, "the impugned state conduct has reached the point at which the values

---

77 *Tessling*, supra note 69 at para. 18.

78 *Ibid* at para. 18.

79 *Ibid* at para. 19.

80 *Tessling*, supra note 69 at para. 23, citing A. F. Westin, *Privacy and Freedom* (1970) at 7.

81 *R. v. Plant*, [1993] 1 SCR 281 at 293.

82 *Duarte*, *supra* note 66 at paras. 18 & 19 ("as a general proposition, surreptitious electronic surveillance of the individual by an agency of the state constitutes an unreasonable search or seizure under s. 8 of the Charter … [O]ne can scarcely imagine a state activity more dangerous to individual privacy than electronic surveillance and to which, in consequence, the protection accorded by s. 8 should be more directly aimed").

83 *R. v. Wong*, [1990] 3 SCR 36 at 43-44 (per La Forest J. for majority).

84 *Tessling*, supra note 69 at para. 19.

85 *Ibid* at para. 42.

underlying contemporary Canadian society dictate that the state must respect the personal privacy of individuals unless it is able to constitutionally justify any interference with that personal privacy."[86]

Relevant considerations in the "totality of circumstances" include, e.g., the place where the search takes place, whether the subject matter of the search was in public view or abandoned, the intrusiveness of the search, and "whether the information was already in the hands of third parties" and if so whether it was "subject to an obligation of confidentiality".[87]

Notably, this last consideration is not definitive. In ***Ward***, the Ontario Court of Appeal expressly recognized the concept of "public privacy":

> …while the public nature of the forum in which an activity occurs will affect the degree of privacy reasonably expected, the public nature of the forum does not eliminate all privacy claims … [I]f the state could unilaterally, and without restraint, gather information to identify individuals engaged in public activities of interest to the state, individual freedom and with it meaningful participation in the democratic process would be curtailed. It is hardly surprising that constant unchecked state surveillance of those engaged in public activities is a feature of many dystopian novels.[88]

Nor does voluntary disclosure to third parties necessarily defeat a reasonable expectation of privacy. Thus, voluntarily surrendering information to a service provider does not definitively nullify a person's privacy interests in relation to state actors, although it is relevant to the reasonableness of any privacy expectation.[89]

b) Reasonableness of the Search

Where a reasonable expectation of privacy exists, the interference with that right must be "reasonable". The gold standard for a reasonable search is the existence of a judicial warrant.

---

86 *Ward*, *supra* note 71 at para. 82.

87 *Tessling, supra* note 69 at para. 32.

88 *Ward*, *supra* note 71 at para 73 and 74.

89 *Ibid* at para. 76.

Warrants are "a means of preventing unjustified searches before they happen, not simply of determining, after the fact, whether they ought to have occurred in the first place."[90] Thus, electronic surveillance is rendered constitutional by "subjecting the power of the state to record our private communications to external restraint and requiring it to be justified by application of an objective criterion."[91] A "detached judicial officer" supplies this external restraint.[92] The Supreme Court has held that "[t]he 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."[93]

Warantless searches "are presumptively unreasonable, absent exigent circumstances".[94] Warantless searches are ***Charter***-compliant only where the government proves that the law authorized the searches, the law itself was reasonable, and the manner of the search was also reasonable.[95]

In its past jurisprudence, the Court has found that law sometimes does authorize searches in at least exigent circumstances. These have in practice usually involved police "safety searches"; that is "carried out in response to dangerous situations created by individuals, to which the police must react 'on the sudden'."[96] This common law rule is reasonable, given the imminence threat to safety.[97]

The Supreme Court has also considered warrantless intercept of private communications under Part VI of the ***Criminal Code***. The warrantless intercept provision, as it then was, permitted warrantless electronic intercepts on an urgent basis to prevent serious and imminent harm.[98] In ***Tse***, the Supreme Court concluded that this provision violated section 8, in large part because the person whose communications were intercepted was never given notice of the intercept. In consequence,

---

90 *Hunter*, *supra* note 76 at 160.

91 *Duarte, supra* note 66 at para. 25.

92 *Ibid*. at para. 25 (noting that "[i]f privacy may be defined as the right of the individual to determine for himself when, how, and to what extent he will release personal information about himself, a reasonable expectation of privacy would seem to demand that an individual may proceed on the assumption that the state may only violate this right by recording private communications on a clandestine basis when it has established to the satisfaction of a *detached judicial office*r that an offence has been or is being committed and that interception of private communications stands to afford evidence of the offence") (emphasis added).

93 *R v. Tse*, 2012 SCC 16 at para. 17.

94 *Tessling*, supra note 69 at para 33.

95 *R. v. Collins*, [1987] 1 S.C.R. 265 at para 23; *R. v. MacDonald*, 2014 SCC 3 at para. 29.

96 *Ibid* at para. 32.

97 *Ibid* at para. 43.

98 *Criminal Code*, *supra* note 23, s.184.4, as interpreted by *R. v. Tse*, *supra* note 93 at para. 27.

> Parliament has failed to provide adequate safeguards to address the issue of accountability ... Unless a criminal prosecution results, the targets of the wiretapping may never learn of the interceptions and will be unable to challenge police use of this power. … In its present form, the provision fails to meet the minimum constitutional standards of s. 8 of the Charter.[99]

This same failure to include a notification regime meant that the impact on the section 8 right was disproportionate to the government's objective of avoiding imminent harm. For this reason, the provision was not saved by section 1 of the Charter.[100]

2. Metadata May Meet the Threshold of Reasonable Expectation of Privacy

I turn now to the application of these principles to CSEC metadata collection. As discussed in Part I, metadata may be enormously revealing of private information; that is, it may amount to what the Supreme Court has called "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[101] It is, therefore, a prime candidate for reasonable expectation of privacy treatment.

While there do not yet appear to be any decided court cases focusing on metadata and the application of section 8, some judgments have focused on related issues; not least, so-called "subscriber information". Here, police in possession of an internet IP address (basically a computer system identifying number) seek and obtain customer identity information associated with this IP from the internet service provider (ISP) to whom the IP belongs. IP addresses can be regarded as a form of metadata associated with internet surfing. The cases to date seem to have turned on the implications of these data being collected, not from the individual or his or her devices directly, but from third-party service providers.

Notably, under the ***Personal Information Protection Electronic Documents Act*** (PIPDEA) (and its provincial equivalents), a business such as an ISP may disclose personal information to a government institution for purposes of law enforcement or where the information may relate to national security, international affairs or national defence.[102] Several lower

---

99 *Tse*, *supra* note 93 at para. 85.

100 *Ibid* at para. 98.

101 *Plant*, *supra* note 81 at 293.

102 *Personal Information Protection and Electronic Documents Act* (PIPEDA), S.C. 2000, c.5, s.7(3)(c.1).

court decisions have considered whether this disclosure of subscriber information to police by ISPs offends ***Charter*** section 8.

At least one such decision tends to suggest that section 8 is not violated, although the Saskatchewan Court of Appeal is that case was badly fractured and the ***ratio*** of the decision is hard to discern.[103] Two other cases, including a second decision from the Saskatchewan Court of Appeal, offer much more nuanced views.

In ***R. v. Ward***, the Ontario Court of Appeal decided that search of subscriber information stripped the accused of "his Internet anonymity" and had the potential "to reveal activities of a personal and private nature".[104] Even so, and even with a strong subjective expectation of privacy, the Court of Appeal doubted the objective reasonableness of the privacy expectation.

At issue in that case was an investigation into child pornography, in which the ISP's services were the vehicle by which the offence was committed. The court gauged the objective expectation of privacy with reference to how a reasonable service provider would respond to a police request in such a case. The reasonably informed person, it concluded, "would accept that it was reasonable for the ISP to make the disclosure requested".[105] The fact that the ISP had the discretion to cooperate with the police in the manner it did under PIPEDA and its terms of service agreement reinforced this conclusion.

However, the Court of Appeal also issued a caution relevant to this article and thus reproduced in full:

> the conclusion in this case is based on the specific circumstances revealed by this record and is not intended to suggest that disclosure of customer information by an ISP can never infringe the customer's reasonable expectation of privacy. If, for example, the ISP disclosed more detailed information, or made the disclosure in relation to an investigation of an offence in which the service was not directly implicated, the reasonable expectation of privacy analysis might yield a different result. Similarly, if there was evidence that the police, armed with the subscriber's name and address, could actually form a detailed picture of the subscriber's Internet usage, a court might well

---

103 *R. v. Spencer*, 2011 SKCA 144

104 *Ward*, *supra* note 71 at paras. 92-93.

105 *Ibid* at para. 105.

> find that the subscriber had a reasonable expectation of privacy.

Ward stands for the proposition, therefore, that metadata may, in fact, attract section 8 protections, and it implies that this likelihood increases in proportion to the sweep of the disclosure and the intimacy of the portrait that might then be painted from the disclosed information.[106]

Moreover, what is reasonable disclosure by an ISP in one instance might not be so reasonable in another. While ISPs may be equally compliant in practice, it does not follow that a court would conclude that acquiesce in a broad, search-of-the-haystack foreign surveillance effort is as reasonable as cooperation in a targeted child pornography police investigation in which the ISP's services are used as a vessel for the crime. In other words, the average user's believe that their metadata are not subject to intelligence trolling via cooperative ISPs may be objectively reasonable.

All told, therefore, ***Ward*** is very poor authority for a CSEC metadata project insulated from section 8 protections. Even less helpful is the majority decision of the Saskatchewan Court of Appeal in ***R. v. Trapp***.[107]

Here, the court concluded that the accused had a reasonable expectation of privacy on facts essentially identical to those in ***Ward***. On the specific question of the ISP and its preparedness to cooperate with police, the majority concluded that a reasonable person might expect the ISP to "exercise a meaningful measure of independent and informed judgment before disclosing information of the kind in question to the police on request", and would be wary in doing so "having regard for the fact information such as this is both confidential and private, and is capable of revealing much about the individual and the individual's online activity in the home."[108] In the end, the accused's challenge in ***Trapp*** failed, but for reasons that are not easily transposable to the CSEC context.[109]

---

106 This is a view apparently also shared by the Alberta Court of Appeal in *Croft*, *supra* note 55. Here, the court held that accused had no (even) subjective expectation of privacy in telephone number subscriber information, distinguishing this type of data from "internet service subscriber information", said to be "the key to the door protecting the privacy of the content of the individual's computer". In comparison, telephone subscriber information could not be used as a link to more content rich data, such as text messages.

107 *R. v. Trapp*, 2011 SKCA 143.

108 *Ibid* at para. 57.

109 The Court ultimately concluded that the police acted reasonably in relying on a *Criminal Code* power – s.487.014 – to obtain data without a court production order. The constitutionality of this provision was not put at issue in the case, but the court felt inclined to affirm that the police had reasonable and probable grounds to believe a criminal offence had been committed and that the ISP had relevant information in its possession. *Ibid* at para. 70. It should not be assumed, therefore, that this provision would exonerate CSEC metadata collection efforts, done for intelligence gathering purpose. It is also worth adding that the Ontario Court of Appeal in *Ward* treated this provision as going to whether a reasonable expectation existed, but refused to view it as "creating

In sum, there is nothing magic about metadata, whether housed with a third party service provider or not. Everything still hinges on the reasonable expectation of privacy. There is little in past court treatment of section 8 to suggest that intelligence surveillance of the sort potentially at issue in the CSEC metadata project lies outside the zone of privacy protected by the ***Charter***. Indeed, the government itself now appears to accept that some metadata collected by CSEC gives rise to a reasonable expectation of privacy.[110]

3. The Present Form of CSEC Metadata Collection May Not Constitute a Reasonable "Search"

If metadata collected by CSEC falls with the constitutional zone of privacy, then CSEC acts unconstitutionally if it collects Canadian metadata unreasonably.

a) Ministerial Authorization Does Not Amount to the Judicial Warrant

The quintessential reasonable search requires judicial authorization. In comparison, the CSEC statute relies on "ministerial authorizations" whenever "private communications" might be collected.

Past CSEC commissioners have apparently considered this rule sufficient to meet ***Charter*** standards. In his 2002–3 report, then Commissioner Claude Bisson noted "before December 2001, CSE would have been in violation of privacy related provisions of both the ***Criminal Code*** and the ***Canadian Charter of Rights and Freedoms*** had it intercepted communications without the certainty that, in doing so, it would not intercept private communications."[111] However, Antonio Lamer, in his 2004–5 report, took the view that the modern regime vitiated this concern: "I am of the opinion that [post-2001 system for ministerial authorization of private communication intercepts] is both reasonable and consistent with other legislation that establishes an authority to engage in activities that would, in the absence of adequate justification, be judged an

---

or extending any police search or seizure power." *Ward*, *supra* note 71 at para. 50. The issue of whether, constitutionally, this sort of provision could extend police (let along intelligence agency) search and seizure provisions is, therefore, a very open question.

110 GOC Response, *supra* note 20, Div 3 at para. 6.

111 Canada, Communications Security Establishment Commissioner, *Annual Report 2002–2003* at 3, n1 < http://www.ocsec-bccst.gc.ca/ann-rpt/2002-2003/role_e.php >.

infringement on the rights of individuals as protected by the ***Charter of Rights and Freedoms***."[112]

It is not clear to me that these commissioners were in a position to consider the sweep of data that is now apparently subject to CSEC intercept. Moreover, Antonio Lamer, at least, seemed to believe the CSEC regime necessary because of the extraterritorial nature of its intercepts – a warrant system could not reach extra-Canadian surveillance. I believe that in a contemporary context, their views require careful reconsideration.

First, since the ministerial authorization regime is aimed at "private communication" it applies, by definition, to a communication with a Canadian nexus. This is not a purely extraterritorial intercept – it is one that risks capturing Canadian communications. There is nothing inherently doubtful about a judge authorizing those intercepts that may capture Canadian-origin communications, even if the latter is embedded in a foreign intelligence collection operation.

Second, it should not be assumed that the categories of "private communications" and information in which a person has a "reasonable expectation of privacy" for ***Charter*** purposes overlap in full. Something may not be private communication, but may still give rise to a reasonable expectation of privacy. The concepts do not move in lock step. Put another way, since the ministerial authorization regime is triggered only when information reaches the level of "private communication", it risks being underinclusive of the data that attract constitutional protection, even assuming it is a proper alternative to a judicial warrant.

Third, I do not believe that it ***is*** an adequate alternative. The section 8 jurisprudence focuses on advance authorization provided by an independent judicial officer, not a political minister. That minister's exact statutory duty under the ***National Defence Act*** is to manage and direct "all matters relating to national defence."[113] As such, he or she is hardly an independent and disinterested reviewer of government search and seizure requests required by the ***Charter***. It is simply impossible to imagine a court honoring the section 8 jurisprudence and viewing an executive actor as a proxy for the impartial judge promised in it.

b) The CSEC Statute Does Not Meet the Standards for Permissible Warantless Intercepts

At issue, therefore, is warrantless interference with privacy. The government's own, recent legal position on CSEC collection is that any search is, nevertheless, reasonable. The intercepts are:

---

[112] Canada, Communications Security Establishment Commissioner, *Annual Report 2004–2005* at 9 < http://www.ocsec-bccst.gc.ca/ann-rpt/2004-2005/activit_e.php >.

[113] NDA, *supra* note 17, s. 4.

- "carried out in the context of foreign intelligence…(not law enforcement)";
- "authorized by the ***National Defence Act*** and, where applicable, through the Ministerial authorizations provided for in the ***National Defence Act;***
- "in furtherance of government objectives of the utmost importance;"
- "minimally intrusive in terms of the type of private information which may be acquired from telecommunications or their Metadata, as well as tailored in scope to the objectives of Part V.I of the ***National Defence Act*** and minimized as much as possible through a variety of privacy safeguards provided for in the ***National Defence Act,*** Ministerial directives, Ministerial authorizations and other applicable policies and procedures".[114]

These arguments do not, however, appear to dovetail with the current jurisprudence on warrantless searches. To date, the government has succeeded in justifying warrantless searches where the law authorizes those measures in ***exigent*** circumstances (with the proviso that the affected individual is then notified of the warrantless search).

Whatever the importance of foreign intelligence, there is nothing in CSEC's law that limits CSEC intercepts to exigent circumstances. Nor is there notification to the affected individual, although here the government might argue that ***ex post facto*** review by the commissioner serves the same purpose.

Boiled to its essence, defence of CSEC's warrantless intercept activity rests on the view that declaring something of national security importance puts it on a different footing than all the other circumstances in which section 8 protects privacy. That is, warrantless intercept is justified by the importance of the issue, and the various prudential measures listed in the government defence backstop a departure from the regular expectations of the ***Charter***.

c) The National Security Imperative Does Not Justify a Departure from Regular Constitutional Expectations

I do not, however, believe this to be a persuasive approach. Certainly, others have argued that national security places search rules on a different

---

[114] GOC Response, *supra* note 20 at Div 3, Pt 2, para 7.

footing than in a conventional law enforcement context.[115] There is some dated and decontextualized judicial musing in support of this view.[116]

But setting aside the issue of whether this argument is best considered as part of the section 8 discussion or instead under section 1, it is not compelling for one simple reason: Canadian practice has already demonstrated unequivocally that national security surveillance need not be treated truly differently from regular police surveillance. The ***CSIS Act*** – dealing with sensitive national security issues – superimposes a full judicial warrant regime on CSIS surveillance activities, in which CSIS persuades a Federal Court judge on "reasonable and probable grounds established by sworn evidence, that a threat to the security of Canada exists and that a warrant is required to enable its investigation".[117]

There is, in other words, nothing foundational about CSEC's national security functions that demand ministerial authorization over a judicial authorization. Nor is there any evident reason why the CSEC approval regime could not draw on the CSIS precedent. Here, a judge would replace the minister in the CSEC authorization process, and that authorization regime extends to the collection of any information in which there is a reasonable expectation of privacy. This would have the welcome effect of preserving the promise and integrity of section 8, while still meeting the government's pressing objectives in relation to foreign intelligence.

In sum, the current ministerial authorization regime under CSEC's law looks much more like expediency than necessity. It is an awkward fix built on doubtful theories about the scope of Canadian privacy law. It deserves no special exemption from the regular constitutional law of the land. Interposing a judge in lieu of a minister would do no violence to CSEC's operations, while at the same time honouring the long-established requirements of the ***Charter***.

Conclusion

In the final analysis, it is difficult to explain why the government has pursued the legal direction suggested by documents released under access law, and in its defence to the current BC Civil Liberties Association challenge to CSEC's law.

---

115 See, e.g., Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis Butterworths, 2005) at 232.

116 *Hunter*, *supra* note 76 at 186 (suggesting, without actually deciding, that the search and seizure standard developed in that case might be different "where state security is involved").

117 *Atwal v. Canada*, [1988] 1 F.C. 107 at para. 36 (FCA), paraphrasing s.21 of the *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23. *Atwal* concluded that this system satisfied section 8.

The prescription offered by this paper is simple: always get ministerial authorizations for metadata collection, even if you personally believe it is not "private communication", and amend CSEC's law to task a judge (in addition or instead of the minister) with authorizing any intercept that may raise reasonable expectations of privacy. Since by the government's own admission, it does not know when information with a Canadian nexus may be swept into its surveillance, prudence suggests that judicial authorization should be sought often.

It is hard to see how either of these suggestions visit real inconvenience on the government. Indeed, civil libertarian critics of these modest proposals might regard them as laughingly formalistic and inadequate.

For my part, I believe that it matters both in principle and practice that judicial authorizations bless intercepts. I agree, however, that the intervention of a judge prior to collection is not alone sufficient protection in the world of Big Data. Other questions – not least on how long government may retain data that forms the Big Data haystack and how it may searched that haystack – are now even more pressing. Those matters are, however, the topic of another article.[118]

The concluding point of this essay is much simpler: the evolution of invasive search and Big Data analysis powers in the hands of the state's intelligence services should not change the existing scope of privacy protections, whether statutory or constitutional. This is a common sense principle that Canadians should reasonably expect a government to honour by instinct, not resist at every turn.

---

[118] For a preliminary discussion of these issues, see Craig Forcese, *The Limits of Reasonableness: The Failures of the Conventional Search and Seizure Paradigm in Information-Rich Environments* (Ottawa: Privacy Commissioner of Canada, July 2011) < http://www.priv.gc.ca/information/research-recherche/2011/forcese_201107_e.asp >.