BUILDING HAYSTACKS: INFORMATION RETENTION AND DATA EXPLOITATION BY THE CANADIAN SECURITY INTELLIGENCE SERVICE

LEAH WEST AND CRAIG FORCESE*

This article examines the technical topic of CSIS's modern data acquisition, retention, and exploitation, a matter not canvassed in the existing legal literature. As part of a special collection on the National Security Act (NSA 2017)*, it focuses on the policy and legal context driving the* NSA 2017 *amendments, relying on primary materials to memorialize this background. This article examines how CSIS has been pulled in divergent directions by its governing law, and sometimes a strained construal of those legal standards, toward controversial information retention practices. It argues that the tempered standards on acquisition, retention, and exploitation of non-threat-related information created by the* NSA 2017 *respond to civil liberties objections. The introduction of the "dataset" regime in the* NSA 2017 *may finally establish an equilibrium between too aggressive an information destruction standard that imperils due process and too constraining an information retention system that undermines CSIS's legitimate intelligence functions. The article flags, however, areas of doubt, the resolution of which will have important implications for the constitutionality and legitimacy of the new system.*

TABLE OF CONTENTS

I. INTRODUCTION

In 2019, Parliament enacted the *National Security Act 2017*[1] and thereby doubled the size of the *Canadian Security Intelligence Act*.[2] By volume, the most significant changes were provisions enabling the Canadian Security Intelligence Service (CSIS or the Service) to

* Leah West is a Lecturer of National Security and Intelligence at the Norman Paterson School of International Affairs, Carleton University. Craig Forcese is a full Professor and Vice-Dean of Graduate Studies at the University of Ottawa, Faculty of Law. The views presented in this article are the authors' alone and do not reflect the opinions of any institution to which they belong.

1 SC 2019, c 13 [*NSA 2017*].

2 RSC 1985, c C-23, as amended by *NSA 2017*, *ibid* [*CSIS Act*].

acquire, retain, and analyze data on "non-threat" actors — that is, data tied to people not believed to pose a threat to the security of Canada.

Some of the legislation's critics argued that the law "expressly empowers mass surveillance [by CSIS] through the collection of bulk data and 'publicly available' data."[3] In this article, we arrive at a different view. The lifeblood of any intelligence service is information. To exploit information, they must be able to acquire, retain, and analyze it. After all, "intelligence" is the end product of this analytical process.[4] Yet, Canada's principal intelligence agency has struggled with the issue of information retention. Indeed, based on what courts have concluded are misapplications of its governing statute, CSIS has swung between two poles: too little retention of information on threat actors and too much retention of non-threat-related information.

This article examines the technical topic of CSIS's modern data acquisition, retention, and exploitation, a matter not canvassed in the existing legal literature. As part of a special collection on the *NSA 2017*, it focuses on the policy and legal context driving the *NSA 2017* amendments, relying on primary materials to memorialize this background. In our analysis, we examine how CSIS has been pulled in divergent directions by its governing law, and sometimes a strained construal of those legal standards, toward controversial information retention practices. We argue the tempered standards on acquisition, retention, and exploitation of non-threat-related information created by the *NSA 2017* respond to civil liberties objections. The introduction of the "dataset" regime in the *NSA 2017* may finally establish an equilibrium between too aggressive an information destruction standard that imperils due process and too constraining an information retention system that could limit CSIS to the business of finding needles in stacks of already discovered needles. We do flag, however, areas of doubt, the resolution of which will have important implications for the constitutionality and legitimacy of the new system.

We proceed in three parts. In Part II, we begin by defining CSIS's mandate, established in 1984 by the *CSIS Act*.[5] In that context, we also explain the difference between "oversight" and "review." Both concepts play an essential role in ensuring CSIS information practices are lawful and respect the *Charter*-protected privacy rights of threat and non-threat actors.

---

3 International Civil Liberties Monitoring Group, "Civil Society Statement Regarding Bill C-59, *An Act Respecting National Security Matters*" (Ottawa: ICLMG, 2018), online: <iclmg.ca/civil-society-statement-c59/>. See also British Columbia Civil Liberties Association, "Written Submissions of the British Columbia Civil Liberties Association ('BCCLA') to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*" (30 January 2018), online: <bccla.org/wp-content/uploads/2018/02/2017-01-30-Written-Submissions-of-the-BCCLA-to-SECU_Bill-C-59.pdf> [BCCLA Submission].

4 Canadian practice distinguishes "intelligence" from "information": "Information" means "data from any source which has not been evaluated but when processed, assessed and analysed, may produce intelligence." "Intelligence," for its part, "means any product resulting from the processing, assessing and analysing of information collected" (Memorandum of Understanding between the Canadian Security Intelligence Service and the Royal Canadian Mounted Police (14 September 2006) at 4, online: *Secret Law Gazette* <secretlaw.omeka.net/items/show/22>). See also Canadian Security Intelligence Service, *Operational Reporting*, CSIS OPS-501 (Ottawa: CSIS, 2010) at 3, online: *Secret Law Gazette* <secretlaw.omeka.net/items/show/48>.

5 *CSIS Act*, *supra* note 2.

In Part III, we outline the impact of a significant Federal Court decision released in 2016 on CSIS's information retention practices.[6] Often referred to as the "ODAC Decision," this judgment arose from a warrant application heard en banc by all the designated judges of the Federal Court. The resulting judgment, authored by Justice Noël, determined that for almost a decade, CSIS erroneously interpreted the scope of its information retention authority and unlawfully retained non-threat-related metadata stemming from the collection (under warrant) of telecommunications ("warranted collection").

In that same Part, we also examine past controversy over CSIS's practice of *not* keeping enough information, specifically, its policy of destroying operational information on CSIS targets. Just as the ODAC decision criticized CSIS for keeping too much information, CSIS's information destruction practice was harshly criticized by the Supreme Court in its 2008 decision of *Charkaoui v. Canada (Citizenship and Immigration)*.[7]

In Part IV, we turn our focus to the reforms enacted by the *NSA 2017*, which, for the first time, grant CSIS the legal authority to acquire, analyze, and retain large quantities of information on non-threat actors ("bulk data"), in the form of "datasets." We examine the policy objective behind this change and consider the operational implications it might have. We then focus on the novel civil liberties and *Charter* issues raised by the acquisition and analysis of data compiled as datasets.

After examining the complex authorization, reporting, and oversight mechanisms built into the dataset regime, we conclude that (for the most part) the *NSA 2017* has checked CSIS's additional powers with considerable new oversight and review requirements. We raise two remaining concerns — areas that should attract close scrutiny by CSIS's oversight and review bodies. We conclude, however, that the *NSA 2017* dataset regime does a credible job in meeting what we (tongue-in-cheek) call the "Spiderman rule" in national security practice: with great power comes great responsibility.

II. CSIS'S INFORMATION COLLECTION MANDATE

CSIS is Canada's domestic security intelligence organization. Since its establishment in 1984, the Service's primary mandate has been to investigate threats to the security of Canada and provide intelligence assessments to the Government of Canada. CSIS also has a foreign intelligence mandate and, to that end, may direct its foreign intelligence activities against non-Canadians within Canada.

The *CSIS Act* sets out a closed list of what constitutes "threats to the security of Canada," commonly summarized as terrorism, espionage and sabotage, foreign influence activities,

6 *X (Re)*, 2016 FC 1105 [ODAC Decision].
7 2008 SCC 38 [*Charkaoui II*].

and subversion.[8] Section 12(1) of the *CSIS Act* sets the parameters for CSIS's intelligence collection when investigating these threats and stipulates:

> The Service shall collect, by investigation or otherwise, to the extent that it is *strictly necessary*, and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada and, in relation thereto, shall report to and advise the Government of Canada.[9]

In contrast, to fulfill its foreign intelligence mandate, section 16 of the *CSIS Act* authorizes "the collection of information or intelligence relating to the capabilities, intentions or activities" of foreign states or persons "within Canada."[10] Aside from the territorial limitation, there are no explicit restrictions on the extent to which CSIS may collect or retain foreign intelligence under the *CSIS Act*. For its part, section 15 permits CSIS to conduct "such investigations as are required for the purpose of providing security assessments" to departments of the Government of Canada as authorized by section 13 of the *CSIS Act*.[11] Again, section 15 does not set any limitations on the type or extent of CSIS's information collection or retention efforts in support of this mandate.

Of course, any search or seizure carried out by CSIS, regardless of the mandate under which it is collected, must also comply with section 8 of the *Charter of Rights and Freedoms*: "Everyone has the right to be secure against unreasonable search or seizure."[12]

Significantly, CSIS does not collect information with the aim of using it to support a criminal conviction; CSIS's role is to analyze the information and provide (often highly classified) security assessments to the Government.[13] Since information collected by CSIS rarely finds its way into a criminal proceeding, the impact of its collection on individual rights is rarely tested in criminal court. This means that without independent "oversight" and robust "review," there is a substantial risk that CSIS could abuse its collection authorities and violate the rights of unwitting Canadians; in fact, avoiding abuse of this kind was precisely the reason why Canada established a professional civilian intelligence agency in the first place.[14]

---

8 *CSIS Act, supra* note 2, s 2.

9 *Ibid* [emphasis added].

10 *Ibid*.

11 *Ibid*.

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

13 In accordance with section 19 of the *CSIS Act*, the Service may, however, share information and intelligence related to criminal activities with law enforcement. Sharing between the agencies, but especially from CSIS to RCMP, is carried out under rigid policy guidelines set out in a document entitled *One Vision 2.0*. See Canadian Security Intelligence Service, *CSIS-RCMP Framework for Cooperation: One Vision 2.0* (Ottawa: CSIS, 2015), online: *Secret Law Gazette* <secretlaw.omeka.net/items/show/21>. See also Colin Freeze, "Concerns Over Bill C-51 Prompt CSIS to Brief Other Agencies on Operations," *The Globe and Mail* (8 September 2016), online: <theglobeandmail.com/news/national/concerns-over-bill-c-51-prompts-csis-to-brief-other-agencies-on-operations/article31788063>.

14 Before the establishment of CSIS, the RCMP's Security Service was responsible for domestic security intelligence. After a series of scandals in the 1970s and 1980s, including the accrual of thousands of files on members of the LGBTQ community in the public service and across Ottawa, the 1981 Commission of Inquiry Concerning Certain Activities of the Royal Canadian Mounted Police recommended that intelligence collection be stripped from the RCMP and entrusted to a civilian intelligence agency with a clearly defined legislative mandate (*Freedom and Security under the Law*, second report, vol 1 (Ottawa: Minister of Supply and Services Canada, 1981) [McDonald Commission]). See also Canadian

The terms "review" and "oversight" are often used interchangeably, but in Canadian practice, these concepts are very different. Put simply, review involves a retrospective performance audit, examining CSIS conduct for compliance with law and policy.[15] Until recently, CSIS conduct was subject to review by the Security Intelligence Review Committee (SIRC). With the passage of the *NSA 2017*, this review responsibility now falls to the National Security Intelligence and Review Agency (NSIRA). With respect to CSIS, NSIRA is mandated to review, among other things, any activity carried out by CSIS, and to investigate complaints made against CSIS.[16] NSIRA must also produce an annual report related to CSIS's warranted collection activities and CSIS's use of "datasets," discussed below.[17] The National Security Intelligence Committee of Parliamentarians, established in 2017, also has a broad mandate to conduct reviews of Canada's intelligence and national security establishments, including CSIS.[18] Both review bodies are entitled to make recommendations regarding CSIS conduct, but, should they find wrongdoing, they have no authority to issue a remedy to those whose rights were violated by CSIS.

Unlike review, oversight involves real-time command and control over the conduct of an organization. It may involve advance approval from an arm's-length body or office before a service proceeds with a course of action. Until the passage of the *NSA 2017*, oversight of CSIS was almost entirely a function of the executive branch, namely the Minister of Public Safety. That said, for both statutory and constitutional reasons, the use of intrusive investigative techniques by CSIS, such as the interception of written, oral, or electronic communication, must be authorized by the Federal Court and has always, therefore, been subject to *ex ante* oversight by independent judges.[19] Moreover, the *NSA 2017* created a new office of the Intelligence Commissioner — a quasi-judicial officer with a crucial new oversight role in CSIS's dataset regime.

III. INFORMATION RETENTION AND ERRONEOUS INTERPRETATIONS OF SECTION 12 OF THE *CSIS ACT*

In the previous section, we outlined the basis upon which CSIS may collect information and intelligence. Sections 12, 15, and 16 of the *CSIS Act* set out the parameters of the purpose for and circumstances in which CSIS may collect information, and who may be the target of a CSIS security intelligence, foreign intelligence, or security assessment investigation. However, in an era defined by big data analytics and the proliferation of

Security Intelligence Service, "History of CSIS" (2 May 2015), online: <web.archive.org/web/20180226033714/http://www.csis-scrs.gc.ca/hstrrtfcts/hstr/index-en.php>; Canada, Library of Parliament Research Branch, *The Canadian Security Intelligence Service*, by Philip Rosen, rev ed (Ottawa: Library of Parliament, 1994).

15 For more on the distinction between review and oversight, see Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Minister of Public Works and Government Services, 2006) at 327–28.

16 *National Security and Intelligence Review Agency Act*, ss 8(1)(c)–(d), being Part I of *NSA 2017*, *supra* note 1.

17 *CSIS Act*, *supra* note 2, ss 11.25, 53(2).

18 *National Security and Intelligence Committee of Parliamentarians Act*, SC 2017, c 15, s 8.

19 *CSIS Act*, *supra* note 2, s 21.

electronic data and communications, the retention of information and the use of that data by the state raises a host of privacy considerations.[20]

We know that CSIS's current "investigational records" data bank includes:

> [P]ersonal information on identifiable individuals whose activities are suspected of constituting threats to the security of Canada; on identifiable individuals who are or were being managed as confidential sources of information; on identifiable individuals no longer investigated by CSIS but whose activities did constitute threats to the security of Canada and which still meet the collection criteria stipulated in section 12 of the *CSIS Act*, and on identifiable individuals the investigation of whom relate to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities.[21]

Variations of this data bank date back to the 1980s.[22] At that time, CSIS urged "it is essential that CSIS collect and retain such information. It is also essential that it have reliable information about groups and individuals who are engaged in activities, or who are in contact with groups and individuals who are engaged in activities which constitute a threat to the security of Canada."[23]

CSIS's retention of information, however, must accord with a limit found within its governing statute: retention of information collected under section 12 must be "strictly necessary." Neither the statute nor the court jurisprudence under it define the term. However, while debating the bill creating CSIS in the House of Commons, Members of Parliament insisted that these words constituted a "clear signal that the mandate is to be interpreted narrowly. Only if it is demonstrably necessary for national security will an investigation be supported by this mandate."[24]

This approach aligned with the findings of the McDonald Commission, the judicial commission of inquiry whose review of the RCMP Security Services sparked the creation of CSIS. In its 1981 report, the Commission warned:

> There is a very widespread fear, both in Canada and in other western democracies, of the dangers to citizens which could result from the improper use of security files. Apprehension about the technical capability of the

---

20 For a general discussion of these issues, see e.g. Paul M Schwartz & Daniel J Solove, "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" (2011) 86:6 NYUL Rev 1814; Fred H Cate, "Government Data Mining: The Need for a Legal Framework" (2008) 43:2 Harv CR-CLL Rev 435; Christopher Slobogin, "Government Data Mining and the Fourth Amendment" (2008) 75:1 U Chicago L Rev 317; Anita Ramasastry, "Lost in Translation? Data Mining, National Security and the 'Adverse Inference' Problem" (2006) 22:4 Santa Clara Comp & High Tech LJ 757; Laura K Donohue, "Anglo-American Privacy and Surveillance" (2006) 96:3 J Crim L & Criminology 1059; Laura K Donohue, "Bulk Metadata Collection: Statutory and Constitutional Considerations" (2014) 37:3 Harv JL & Pub Pol'y 757.

21 Canadian Security Intelligence Service, "Info Source: Sources of Federal Government and Employee Information," (5 June 2018), online: *Government of Canada* <canada.ca/en/security-intelligence-service/corporate/transparency/access-to-information-and-privacy/info-source.html>.

22 See *Zanganeh v Canada (Canadian Security Intelligence Service)*, [1989] 1 FC 244 at 251.

23 *Ibid* (Affidavit, CSIS).

24 *House of Commons Debates*, 32-2, No 2 (10 February 1984) at 1274 (Robert Kaplan), cited in *Swan v Canada (TD)*, [1990] 2 FC 409 at 424–25; ODAC Decision, *supra* note 6 at para 137. See also ODAC Decision, *ibid* at paras 50–55, 133.

> modern state to look into every nook and cranny of its citizens' lives and to retain, for unknown purposes, mountains of information about us all is reflected in the oft-heard phrase "they must have a file on me".
>
> …
>
> We believe that controls are needed to prevent a security intelligence agency from maintaining files on thousands of people who are not threats or potential threats to the security of Canada. To say that the agency can collect information regarding individuals as long as this information relates to the agency's mandate is so vague and loose a rule as to justify almost any collection programme.[25]

A. RETAINING TOO LITTLE THREAT-RELATED INFORMATION

1. DESTROYING INFORMATION "TO PROTECT CIVIL LIBERTIES"

Cognizant of these political concerns leading to its creation, CSIS applied the "strictly necessary" standard not only to its decision to commence investigations, but also its retention of information. In 2009, then-CSIS director Richard Fadden noted that CSIS operated on the assumption that "to protect civil liberties, we would only retain what we strictly needed in order to do our jobs."[26] One interpretation of the *CSIS Act*'s "strictly necessary" standard was codified as CSIS Policy OPS-217, governing the handling and retention of operational notes. The policy stipulated that employees must destroy notes following transcription into a report, and only retain them where "information contained in the notes may be crucial to the investigation of an unlawful act of a serious nature and employees may require their notes to refresh their memories prior to recounting the facts of an event."[27]

Even where this policy threshold for retention was met, CSIS tilted toward destruction rather than retention. The 2010 report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 (the Air India Commission) criticized CSIS's cautious information-handling practices in the period after the 1985 terrorist bombing of Air India Flight 182.[28] The downing of Flight 182 was the largest act of aviation terrorism before 9/11 and remains the deadliest terrorist attack in Canadian history. Tragically, CSIS and RCMP badly mismanaged the investigations both before and after the attack. Among other things, the Commission found that CSIS destroyed operational notes relevant to the Air India bombing investigation and its subsequent prosecution, notwithstanding a policy that "notes had to be preserved in cases that might result in prosecutions where CSIS evidence would

---

25 McDonald Commission, *supra* note 14 at 518.

26 Richard B Fadden, Address (Remarks delivered at the Canadian Association for Security and Intelligence Studies (CASIS) Annual International Conference, 29 October 2009), online: [web.archive.org/web/20131016230315/http://www.csis-scrs.gc.ca/nwsrm/spchs/spch29102009-eng.asp] [Fadden 2009].

27 Canadian Security Intelligence Service, CSIS Policy OPS-217 (Ottawa: CSIS) at para 3.5, cited in *Charkaoui II*, *supra* note 7 at para 35.

28 Canada, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy, Volume 2, Part 2: Post-Bombing* (Ottawa: Minister of Public Works and Government Services, 2010), online: <publications.gc.ca/collections/collection_2010/bcp-pco/CP32-89-2-2010-1-eng.pdf> [Air India Commission].

be necessary."[29] CSIS also destroyed recordings of telephone calls intercepted under warrant. These tapes "were routinely erased without considering whether that was a sound practice in light of terrorist attacks on Air India Flight 182 and at Narita [International Airport]."[30] CSIS in effect defended this destruction as "conforming to policy, regardless of whether the policy was appropriate to the circumstances."[31]

The Commission disagreed, and condemned CSIS's practices, concluding "it was a serious deficiency for CSIS to continue to destroy its notes and recordings, either ignoring its own policies or not taking care to ensure that its policies would not hinder criminal investigations and prosecutions for terrorism offences."[32]

2. Destroying Information at the Expense of Due Process

The Air India Commission was not the first accountability body to raise concerns about CSIS's information destruction practices. While the Air India Commission was preoccupied with the destruction of information that might have evidential value in a criminal prosecution, CSIS's review body, SIRC, raised slightly different due process issues. As early as 2005, SIRC expressed concern with CSIS's practice of destroying operational notes taken by investigators during security screening assessments used to support decisions on whether an official should receive security clearance. In SIRC's words:

> The issue of what was said during security screening interviews is a perennial source of argument in the course of the Review Committee's investigation of complaints. Complainants frequently allege that the investigator's report of their interview is not accurate: that their answers are incomplete, or have been distorted or taken out of context. *Even if there were a security concern with allowing a complainant to review notes of questions that were asked and answers given at the interview, there is no reason why such notes could not be preserved for a reasonable period so that they are available to the Review Committee* in the event of a complaint in respect of the security screening activity in question.[33]

The tension between due process and CSIS's information destruction practices reached the Supreme Court of Canada in yet another type of proceeding — immigration security certificates issued under Canadian immigration law. The key decision — popularly known as *Charkaoui II* — stemmed from the destruction of operational notes collected during interviews with Adil Charkaoui, a non-citizen, who became the subject of an immigration security certificate. That process led to lengthy detention and his possible removal from Canada. CSIS summaries and the reports founded on those notes formed the basis for the certificate. However, without original operational notes, there was no way for the Minister who issued the security certificate, or a court on judicial review, to verify the information in these documents.[34]

---

29 *Ibid* at 474.
30 *Ibid* at 466.
31 *Ibid*.
32 *Ibid* at 475.
33 *Liddar v Deputy Head of the Department of Foreign Affairs and International Trade*, File No 1170/LIDD/04, 7 June 2005, at para 72, cited in *Charkaoui II*, *supra* note 7 at para 40 [emphasis in original].
34 *Charkaoui II*, *ibid* at para 39.

In *Charkaoui II*, the Supreme Court reviewed CSIS's Policy OPS-217 governing the destruction of operational notes. It acknowledged "the confidential nature of operational notes, which, if compromised, could cause injury to the national interest or harm to an individual affected by their content."[35] Nevertheless, the Supreme Court concluded that the policy was built "on an erroneous interpretation" of the *CSIS Act*: "[I]n our view, s. 12 of the *CSIS Act* demands that it retain its operational notes. To paraphrase s. 12, CSIS must acquire information to the extent that it is strictly necessary in order to carry out its mandate, and must then analyse and retain relevant information and intelligence."[36] Consequently, "as a result of s. 12 of the *CSIS Act*, and for practical reasons, CSIS officers must retain their operational notes when conducting investigations that are not of a general nature. Whenever CSIS conducts an investigation that targets a particular individual or group, it may have to pass the information on to external authorities or to a court."[37]

The Supreme Court found that CSIS investigations may affect an individual's right to life, liberty, and security of the person protected under section 7 of the *Charter*; this is certainly the case in the context of an immigration security certificate.[38] As such, the destruction of operational notes violated the procedural rights owed to Charkaoui, and CSIS's duty to retain and disclose information.[39] While the Supreme Court denied the applicant's request for a stay of proceedings, it held that the appropriate remedy was to recognize a duty to disclose.[40]

The Supreme Court's decision clearly surprised CSIS. The agency saw virtue in its information destruction policies. As the Air India Commission concluded, these rules distanced CSIS from its tarnished predecessor, the RCMP Security Service. In the Air India Commission's words, CSIS "rightly sought to chart a path distinct from law enforcement. This entailed a greater respect for the privacy of their targets than that employed by the RCMP Security Service."[41] Director Fadden also advanced this rights-affirming view in 2009, urging that "[o]ur *Act* instructed us to collect/retain information that was 'strictly necessary' in order to determine if a person was a threat. This was seen as *protecting* civil liberties."[42]

Director Fadden suggested that *Charkaoui II* was emblematic of the "turbulent legal environment in which CSIS finds itself."[43] Because of this decision, he concluded, CSIS "must now retain all operational material — such as notes, electronic surveillance and other data — related to cases that could involve future litigation. Because it is difficult to predict what an investigation will lead to, we have made the decision to retain virtually all the information we collect."[44] Retaining everything, he observed, "is now seen as the best defence of civil liberties. I am not sure if Canadians or even our national security community can foresee the full effects of this decision."[45] The Director predicted, "within several years,

35 *Ibid* at para 32.
36 *Ibid* at para 38.
37 *Ibid* at para 43.
38 *Ibid* at para 53.
39 *Ibid* at paras 62, 64.
40 *Ibid* at para 77.
41 Air India Commission, *supra* note 28 at 449.
42 Fadden 2009, *supra* note 26 [emphasis in original].
43 *Ibid*.
44 *Ibid*.
45 *Ibid*.

someone will accuse us of acting like the Stasi because of the information we are now compelled to keep."[46]

B. RETAINING TOO MUCH NON-THREAT-RELATED INFORMATION

Less than a decade later, the stockpiling of information by CSIS was indeed in the spotlight. The concerns raised in 2016 were not, however, connected to information retention practices mandated by the Supreme Court. Instead, the criticisms were directed at CSIS's practice of indefinitely retaining non-threat-related personal information: a practice underway at CSIS even before the *Charkaoui II* decision.

During its lawful investigations, it is common for CSIS to collect so-called "third-party information" — that is, information unrelated to a threat. Third-party information is, and has always been, at risk of collection in intelligence investigations, but the risk of incidental collection is heightened when large volumes of electronic information are involved. As a banal example, imagine that CSIS has authority to wiretap a target who telephones a pizza parlour; CSIS will inevitably collect statements made by the restaurant's employee who takes his order. The employee is not a target, and as such his comments are considered "third-party" information.

When created, CSIS inherited the RCMP's Technical Aids Policy and Procedure Manual. That document, and related ministerial directions, established that recorded intercepts of "innocent" third parties and any other "non-target" would generally be destroyed, unless they formed part of "Master Evidentiary" tapes.[47] These law enforcement practices were carried over to CSIS, but instead of preserving tapes for evidential purposes, CSIS retained recordings of third parties (unevenly, as it turned out) if they revealed significant "subversive activity."[48] This practice was broadly consistent with CSIS's ultimate conclusion that information retention in section 12 investigations needed to meet the "strictly necessary" standard.

Technology, however, changed the nature and potential intelligence value of third-party information. That information was now amenable to being machine-queried to derive new intelligence insights. As the Federal Court would ultimately find, "[i]n the early 2000's, the CSIS considered that the information it collected through investigations was underutilised as it was not processed through modern analytical techniques."[49]

1. METADATA AND DATA ANALYTICS

By the mid-2000s, the technological environment for intelligence work had changed dramatically. Although unrelated to CSIS itself, the story of the Rafic Hariri investigation is as good a bellwether of this trend as any other. On 14 February 2005, Hariri, the former Prime Minister of Lebanon, was assassinated in a truck bombing. In response, the United

---

46 *Ibid*.
47 Air India Commission, *supra* note 28 at 439.
48 *Ibid* at 442.
49 ODAC Decision, *supra* note 6 at para 37.

Nations and Lebanon created a Special Tribunal to prosecute those responsible.[50] Since then, five members of Hezbollah have been indicted, and trials *in absentia* began in 2014.[51]

These investigations leveraged an innovative technical tool: a Lebanese police captain, Wissam Eid, pursued the relatively novel idea of focusing on metadata accumulated by cellphone companies. Metadata is "data about data" — that is, it is the contextual information that surrounds the content of digital communication.[52] It includes, among other things, the date and time of a call, the length of the call, and the location of the device at the time of the call. With a court order, Eid reviewed call and text message records for the four months up to the assassination and identified a cluster of cellphones following Hariri. Investigators ultimately linked these phones to senior members of Hezbollah. Eid was himself assassinated by a car bomb on 25 January 2008. However, Lebanese authorities transferred Eid's work to the UN investigators, who pieced together a jigsaw puzzle of connections from the metadata, paving the way to the ultimate indictments.[53]

Eid's work demonstrated the power of metadata and of big data analytic techniques to piece together intelligence-rich mosaics from the data debris we scatter around us while leading increasingly connected lives. When the CSIS director referred to the Stasi in 2009, the iPhone was only two years old. That year, 14 percent of Canadians had smartphones; by 2016, that number had increased to 76 percent.[54] That same year, nearly all Canadians under 45 used the Internet every day.[55] These practices, and more generally the digitization of data, create haystacks of information in which intelligence services increasingly wish to search for patterns not just furthering investigations of known threats, but also potentially revealing unknown threats.

These data also provide intelligence analysts with a "feast" in an era where, because of cryptographic technology, traditional forms of information gathering like the telephone wiretap are increasingly in "famine." Ubiquitous data encryption makes the content of some communications and digitized information inaccessible, even when a judicial warrant duly authorizes the interception of those communications. In 2018, the Australian Federal Police reported that "[o]ver 90% of telecommunications information being lawfully intercepted … now uses some form of encryption. Malicious actors increasingly communicate through secure messaging applications, social media and Voice over Internet Protocol (VoIP) services."[56] Closer to home, a 2018 RCMP briefing memorandum reported "[a]pproximately

---

50 See Ronen Bergman, "The Hezbollah Connection," *The New York Times Magazine* (10 February 2015), online: <nytimes.com/2015/02/15/magazine/the-hezbollah-connection.html>.

51 *Ibid*.

52 Michael Geist, "Why Watching the Watchers Isn't Enough: Canadian Surveillance Law in the Post-Snowden Era" in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: University of Ottawa Press, 2015) 225 at 229–30.

53 Bergman, *supra* note 50 (albeit the indictments were brought before a mixed Lebanese/international tribunal process that by this writing had little else to show for its efforts).

54 Statista, "Penetration of Mobile Devices in Canada as Share of the Population from 2009 to 2016," online: <statista.com/statistics/462386/mobile-device-penetration-canada/>; Statistics Canada, "The Internet and Digital Technology" (14 November 2017), online: <www150.statcan.gc.ca/n1/pub/11-627-m/11-627-m2017032-eng.htm>.

55 Statistics Canada, *ibid*.

56 Austl, Commonwealth, House of Representatives, *Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018* (Explanatory Memorandum) (Canberra: Minister for Home Affairs, 2018) at para 3, online: <parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6195_ems_1139bfde-17f3-4538-b2b2-5875f5881239/upload_pdf/685255.pdf>.

70 per cent of all communications intercepted by CSIS and the RCMP are now encrypted … 80 organized crime groups were identified as using encryption in 2016 alone."[57] Canadian security services have described encrypted communication — and the resulting "going dark" phenomenon — as one of the most serious challenges they face.[58]

2. OPERATIONAL DATA ANALYSIS CENTRE

In this environment, it is not surprising that CSIS seeks to exploit metadata for intelligence purposes. In 2005, a CSIS taskforce recommended the Service "retain all data collected from investigations and warrants in order to exploit that information in ongoing and future investigations through a technological program."[59] Subsequently, in April 2006, CSIS created the Operational Data Analysis Centre (ODAC). The ODAC serves as the "centre for excellence for the exploitation and analysis" of a number of databases incorporating, among other things, third-party information collected under warrant.[60]

The warrants under which that data was collected obliged CSIS to review third-party information to determine whether it met standards for retention. CSIS retained information — including third-party information — where it had reasonable grounds to believe the information "may assist" in a section 12 or section 16 investigation — a standard significantly more relaxed than "strictly necessary."

Applying this threshold, the contents of third-party communications were routinely destroyed. CSIS distinguished, however, between the content of communications and so-called "associated data." Associated data included all metadata acquired from communications service providers, regardless of whether it was attributable to a target or a third party.[61] CSIS retained associated data — including third-party information — even where the content with which it was associated "was assessed as unrelated to threats and of no use to an investigation, prosecution, national defense, or international affairs."[62] Put another way, CSIS kept associated data because it "may assist" in its general data analytics efforts.

From 2006 forward, associated data was "retained and inserted into the ODAC program for future investigative purposes."[63] ODAC manages

> a powerful program which processes metadata resulting in a product imbued with a degree of insight otherwise impossible to glean from simply looking at granular numbers.…The end product is intelligence which reveals specific, intimate details on the life and environment of the persons the CSIS investigates. The

---

57 Catharine Tunney, "RCMP's Ability to Police Digital Realm 'Rapidly Declining,' Commissioner Warned," *CBC News* (24 September 2018), online: <cbc.ca/news/politics/lucki-briefing-binde-cybercrime-1.4831340>.

58 See e.g. Intrepid Podcast, "Episode 36: CSIS Director David Vigneault," online (podcast): <intrepid podcast.com/podcast/2018/5/11/t7a66ktq1pwmscgk9hinevyhu3slcn>.

59 ODAC Decision, *supra* note 6 at para 11.

60 *Ibid* at para 37.

61 *Ibid* at paras 13, 31.

62 *Ibid* at para 33.

63 *Ibid* at para 35.

> program is capable of drawing links between various sources and enormous amounts of data that no human being would be capable of.[64]

CSIS believes that "by harnessing available data through advanced analytics, it will increasingly be able to predict the behaviour of targets, generate new investigative leads, uncover networks, and make more informed decisions regarding the placement of surveillance resources, among other investigative benefits."[65]

SIRC reviewed ODAC for the first time in its 2014–2015 Annual Report. It cautioned that the full scope of ODAC was likely not understood by the Federal Court, the entity that had issued the warrants that authorized and also constrained the collection of associated data. SIRC recommended CSIS make the Federal Court aware "of the particulars of the Service's retention and use of metadata collected under warrant."[66] CSIS rejected this recommendation, and SIRC did not have the power to issue a remedy or compel action on the part of CSIS.

However, the Federal Court was attentive to the SIRC report, when made public. In response, it constituted an en banc hearing of all designated judges authorized to hear CSIS warrant applications. The hearing addressed proposed amendments to the conditions templates included in CSIS warrants and the associated data collection and retention program. This hearing was not technically an ex post facto review of CSIS's conduct in carrying out searches authorized by the Court, as is common in a criminal proceeding where the Crown seeks to admit as evidence information derived from a search. Nonetheless, the procedure had a similar effect, and exemplified how the combination of review and judicial oversight can work to correct and constrain the actions of intelligence officials.

In authoring the resulting decision, Justice Noël chastised CSIS and its legal counsel for failing to apprise the judges of the full scope of associated data retention.[67] More critically for this article, the Federal Court found that CSIS had once again based its program on an erroneous interpretation of the "strictly necessary" qualifier in section 12. The Court concluded that the strictly necessary qualifier controls not only the scope of collection but also the standards for retention: "[I]f collection of information is performed on a strictly necessary basis, it goes without saying that retaining the strictly filtered information is permitted because the point of entry of the information is the strict collection process. Therefore, the retention function may only logically retain what has been collected in a 'strictly necessary' manner."[68] Section 12 could not, therefore, authorize retention of third-party associated data:

> [I]t is crucial to distinguish that incidental collection of non-target and non-threat related information does not form part of what is "strictly necessary" to collect. Therefore, non-target and non-threat third party information may only be retained for a short period of time in order to ensure that it is not related to national

---

64 *Ibid* at para 42.

65 Security Intelligence Review Committee, *Broader Horizons: Preparing the Groundwork for Change in Security Intelligence Review*, 2014–2015 Annual Report (Ottawa: Public Works and Government Services Canada, 2015) at 25, online: <www.sirc-csars.gc.ca/pdfs/ar_2014-2015-eng.pdf> [SIRC 2014–2015].

66 *Ibid*.

67 ODAC Decision, *supra* note 6 at para 108.

68 *Ibid* at para 185.

> security. If, after such short time period, the information is determined not to be related to threats to the security of Canada … or of assistance to a prosecution, to national defence or international affairs, it must be destroyed.[69]

The Court concluded that the ODAC associated data retention program was unlawful under CSIS's statute: "CSIS cannot retain associated data as it is not empowered by law to do so, in plain words, it has no jurisdiction to do so."[70] Regrettably, the Federal Court never reached the constitutional issues raised by CSIS's retention and use of third-party associated data, and specifically whether the ODAC practice violated section 8 of the *Charter*.[71]

3. IMPLICATIONS

After the ODAC Decision, CSIS was confronted with Supreme Court and Federal Court decisions seemingly counselling different approaches to CSIS's information retention obligations. Indeed, at first blush, the Federal Court's application of the "strictly necessary" standard to retention appears inconsistent with the Supreme Court's holding in *Charkaoui II*, and its requirement that information *be* retained, even when not "strictly necessary" to an intelligence investigation. However, the Federal Court noted (correctly) that *Charkaoui II* concerned target information — that is, information CSIS can lawfully collect intentionally on a target — and not non-threat-related, third-party, incidentally collected information. Put another way, the Supreme Court was dealing with the retention of information CSIS lawfully acquired in a targeted process. The Supreme Court favoured retention of this information. In comparison, the Federal Court was confronted with the data "by-catch" — collateral information accidentally scooped up in the legal pursuit of a target. For this by-catch, Justice Noël concluded, the policy must be one of "catch and destroy."

These different outcomes were also consistent with the different legal issues at stake in the two cases. *Charkaoui II* demanded retention because the information was threat-related and might then have due process implications for legal proceedings related to the subject of the threat investigation. Third-party "associated data" did not raise those same concerns — this was information about non-threats retained in the hopes of revealing something unknowable. To justify retention of associated data on the holding of *Charkaoui II* would be, therefore, to miss this key distinguishing point. Its practical effect would be to de-link rules on retention from any statutory limitation whatsoever. It would mean that whatever CSIS had, it could keep, even if the information concerned innocent people incidentally caught in an intelligence investigation, so long as there was an argument to make that it might one day assist in a threat investigation. This approach — and not the one imposed by *Charkaoui II*

---

69 *Ibid* at para 186.

70 *Ibid* at para 197.

71 Arguably, however, the Federal Court deemed the inclusion of warrant conditions requiring the destruction of non-threat-related information necessary to ensure that CSIS's warranted collection activities were themselves "reasonable." Whether ignoring those conditions and indefinitely retaining associated data was sufficient to render the warranted collection unconstitutional is an argument for another article.

— was more likely to attract analogies comparing CSIS to the Stasi. Indeed, the public reaction to the revelations in the Federal Court decision was fierce.[72]

4. THE GAP

Still, the Federal Court holding that CSIS could only keep non-target information, where its retention was "strictly necessary" to advance a security intelligence investigation had implications for more than just the "associated data" at issue in the ODAC Decision. Its findings suggested that any project undertaken by CSIS that relied on the acquisition or aggregation of non-threat-related information would fail to meet the strictly necessary standard and could not lawfully continue. This potentially disallowed any form of data analytics that required the aggregation of large volumes of information to identify a potential threat. Taken to its logical extreme, CSIS would violate its statute were it to retain 411.ca on its computers.

Justice Noël acknowledged the operational implications of his decision on CSIS's capacity to engage in this modern intelligence practice, but affirmed that this was what the antiquated statute required:

> [T]he *CSIS Act* is showing its age. World order is constantly in flux; for example state cyber-attacks are a novel form of war and a new era of the old Cold War is appearing. In addition, terrorist attacks are deeply hurting innocent civilians across the world, technology evolves rapidly, and priorities and opinions change. Canada can only gain from weighing such important issues once again. Canadian intelligence agencies should be provided the proper tools for their operations but the public must be knowledgeable of some of their ways of operating.
>
> …
>
> Although I have determined in these reasons that the retention of associated data falls outside the legal scope of the *CSIS Act*, I think it important for future debates to note that evidence was produced establishing that the processing and analysis of associated data has yielded some useful intelligence results. In some cases, analysis of retained data in past cases indeed contributed to new investigative leads and other useful pertinent information.[73]

---

[72] Indeed, an editorial in the Globe and Mail addressing CSIS and bulk data collection noted "[n]o one wants a Stasi-type secret service" ("We Need to Talk About Bulk Data," The Globe and Mail (10 January 2017) A12). Overall, there was considerable coverage of the ODAC decision in the media. "Canadian Newsstand," a subscription-based database of leading Canadian print dailies now called "Canadian Newsstream," shows 15 stories on "CSIS" "illegally" "retained" in November 2016, the month the Federal Court decision was released (online: <https://www.proquest.com/products-services/canadian_newsstand.html>).

[73] ODAC Decision, *supra* note 6 at paras 264–65.

IV. IN SEARCH OF BALANCE: THE CSIS "DATASET" REGIME

A. THE SECURITY OBJECTIVE

Caught between the standards in *Charkaoui II* and the ODAC Decision, CSIS became an agency (1) mandated to retain indefinitely personal information related to its targets if there were a chance its investigation would lead to legal proceedings, but (2) without the authority to retain any non-threat-related information needed to conduct modern data analytics.[74] Put another way, CSIS could use modern analytic techniques to search for needles, but only in the lawfully retained databases comprising already collected needles. Amendments to the *CSIS Act* brought about in the *NSA 2017* reversed the implications of the ODAC Decision and gave CSIS the authority to lawfully engage in the acquisition, retention, and analysis of non-threat-related information.

To be clear: the legislative changes did not broaden CSIS's formal investigative powers. CSIS, for example, cannot now investigate a threat to the security of Canada on a more relaxed standard. CSIS does not have more invasive powers to collect information. Its grounds for seeking a warrant to lawfully access communications do not change. Nor does the legislation eliminate the "strictly necessary" threshold as it applies to the collection and retention of threat information. Instead, the amendments establish a separate and distinct regime for the acquisition, retention, and analysis of datasets that are likely to assist in the execution of its duties and functions under the *CSIS Act*. To return to a haystack analogy: under its original *Act*, CSIS could conduct threat investigations of a haystack to the extent "strictly necessary" to a threat investigation, and could keep the needles it found, also to the extent strictly necessary. After the ODAC Decision, it could not keep any of the hay that might have been scooped up incidentally while collecting the needle. After the *NSA 2017*, CSIS may retain this hay. Even more critically, it may also build its own bespoke haystack of data within CSIS to figure out where to search for new needles. That is, CSIS may now acquire, retain, and analyze "datasets" of personal information that, in the parlance of the ODAC Decision, is non-threat-related, third-party information.

When introducing the *NSA 2017*, the government stated that

> [t]oday's threats to Canada's national security are fast, complex and dynamic, and threat actors are highly connected and mobile. The ease of movement across international borders and spread of social media networks and modern communications technology can be used by individuals and groups seeking to harm Canada. This creates some very real challenges for CSIS.[75]

---

74 This consequence was reflected by SIRC in its 2017–2018 annual report. That year, SIRC reviewed the measures taken by CSIS following the ODAC decision and found that "there is a risk that CSIS could exceed its existing legislative authorities in the retention of non-threat-related information on individuals not suspected of constituting a threat to national security" (Security Intelligence Review Committee, *Building for Tomorrow: The Future of Security Intelligence Accountability in Canada*, 2017–2018 Annual Report (Ottawa: Public Services and Procurement Canada, 2018) at 29, online: <sirc-csars.gc.ca/pdfs/ar_2017-2018-eng.pdf> [SIRC 2017–2018]).

75 Canadian Security Intelligence Service, "Amendments to the *CSIS Act* – Data Analytics" (20 June 2017), online: *Government of Canada* <canada.ca/en/security-intelligence-service/news/2017/06/amendments_to_thecsisact-dataanalytics.html>.

The government believed CSIS needed a new authority to collect data and deploy modern analytics tools to filter through the vast electronic universe threat actors use to conduct and mask their activities.

Whether CSIS will have the capacity to do this searching effectively is an open question. SIRC was wary of CSIS data analytics capabilities in the past. In SIRC's 2014–2015 annual report, for example, it noted CSIS "lacked precise data on the program's efficiency and effectiveness."[76] In its 2017–2018 annual report, SIRC expressed skepticism of the operational value of CSIS bulk datasets containing third-party, non-target data.[77]

CSIS disagreed, however, with SIRC's conclusion and questioned the review body's assessment methodology.[78] CSIS has urged it is "developing a system for assessing the utility of individual datasets and for integrating these assessments into decisions regarding the retention of a dataset. The record keeping requirements under [the *NSA 2017*], along with enhanced storage and analytic systems, will allow for additional validation of retained datasets based on operational utility."[79]

Given these differing views, we are not able to assess how vital bulk data analytics will be to CSIS once implemented. We find instructive, however, the 2016 review of bulk dataset exploitation by UK intelligence services, conducted by the then-independent reviewer of anti-terrorism laws, David Anderson. The UK understanding of this "bulk personal dataset" also describes what is at issue in Canada under the *NSA 2017*:

> [A bulk personal dataset] includes personal data relating to a number of individuals, and the nature of that set is such that the majority of individuals contained within it are not, and are unlikely to become, of interest to the [intelligence services] in the exercise of their statutory functions. Typically these datasets are very large, and of a size which means they cannot be processed manually.[80]

> UK agencies urge bulk personal datasets (BPDs) enable
>
> the security and intelligence agencies to focus their efforts on individuals who threaten our national security or may be of other intelligence interest, by helping to identify such individuals without using more intrusive investigative techniques. It helps to establish links between subjects of interest or better understand a subject of interest's behaviour. BPD also assists with the verification of information obtained through other sources (for example agents) during the course of an investigation or intelligence operation.
>
> ...

---

76 SIRC, 2014–2015, *supra* note 65 at 25.
77 SIRC, 2017–2018, *supra* note 74 at 30.
78 *Ibid* at 33.
79 *Ibid*.
80 UK, Home Office, *Security and Intelligence Agencies' Retention and Use of Bulk Personal Datasets* (Draft Code of Practice) (London: Home Office, 2016) at para 2.2, online: <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/557860/IP_Bill_-_Draft_BPD_code_of_practice.pdf>.

> Using BPD also enables the security and intelligence agencies to use their resources more proportionately because it helps them exclude potential suspects from more intrusive investigations.[81]

The independent reviewer examined UK security agency operational use of datasets through several case studies. In his assessment, the case studies "provided unequivocal evidence of [BPDs'] value. Their principal utility lies in the identification and development of targets, although the use of BPDs may also enable swift action to be taken to counter a threat."[82] BPDs were used for many purposes, including identifying potential terrorists and agents, preventing imminent travel, and prioritizing intelligence agency work. In the reviewer's assessment,

> [i]t will often be possible, in a given instance, to identify an alternative technique that could have been used. However many such alternatives would be slower, less comprehensive or more intrusive.… In some areas, particularly pattern analysis and anomaly detection, no practicable alternative to the use of BPDs exists. These areas of work are vital, since they can provide information about a threat in the absence of any other intelligence seed.[83]

B. THE CIVIL LIBERTIES QUESTIONS

Still, even if one accepts the intelligence value or the necessity of these programs, the question becomes one of balance. A key issue is whether CSIS can leverage data on Canadians to investigate threats without creating a disproportionate risk, or indeed even the perception, that CSIS "must have a file" on all of us.

Following the introduction of the *NSA 2017*, several civil society groups condemned the dataset regime, describing it as "an activity that constitutes mass surveillance of Canadians."[84] They argued that all data collection should meet the strictly necessary standard set out under section 12 of the *CSIS Act* and should only be employed where no less intrusive means of collection are available.[85] A subtext in some of the objections was that CSIS would use its new dataset system improperly, perhaps to single out minorities — that is, to engage in ethnic profiling.

Both concerns deserve consideration. First, ethnic profiling is a perennial preoccupation, especially since 9/11. It is not always clear what those who use the expression mean by "ethnic profiling," a colloquial term. However, profiling includes, at minimum, directing investigative resources at racial, religious, or ethnic groups because of those qualities, and not because of indicators tied to actual threat considerations. CSIS has repeatedly reported it

> does not base its security intelligence investigations on racial, religious or ethnic profiling. Rigorous targeting and warrant application processes are currently in place, involving both internal oversight mechanisms, and

---

81 UK, Prime Minister, *Report of the Bulk Powers Review*, by David Anderson (London: Crown, 2016) at para 8.2, online: <assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/546925/56730_Cm9326_WEB.PDF> [Anderson Report].

82 *Ibid* at para 8.33.

83 *Ibid* at paras 8.35–8.36.

84 See e.g. BCCLA Submission, *supra* note 3 at 1.

85 *Ibid*.

> independent external review by independent counsel with the Department of Justice, the Minister of Public Safety and the Federal Court of Canada. Finally, the *CSIS Act* provides for review by SIRC of any activity undertaken by CSIS to ensure compliance with policy, ministerial direction and Canadian law. Together, these mechanisms have made CSIS the most externally reviewed intelligence service in the world.[86]

These denials have not satisfied critics, who may point to evidence of biased conduct by CSIS. We cannot resolve this issue in this article. The more material issue, however, is whether new dataset powers might contribute to biased investigations, perhaps even without CSIS's conscious realization. The answer to that question is one of process: CSIS denies a policy of biased investigations. Confirming its practices (in relation to datasets or in the exercise of any other power) are not, in fact, biased depends on oversight and review. In the dataset context, that oversight and review must be attentive to new questions of algorithmic bias, a matter to which we return.

Second, there is confusion between the collection of datasets with "mass surveillance" (or "dragnet surveillance"). This approach conflates the availability of data (datasets) with its actual use (surveillance), treating use as following automatically from availability. The difference between the availability of collected and archived data and a permanent, panoptic form of surveillance is a distinction without a difference for some analysts.[87] In comparison, David Anderson viewed the difference as compelling in his 2016 report on bulk powers:

> [I]t should be plain that the collection and retention of data in bulk does not equate to so-called "*mass surveillance*". Any legal system worth the name will incorporate limitations and safeguards designed precisely to ensure that access to stores of sensitive data (whether held by the Government or by communications service providers [CSPs]) is not given on an indiscriminate or unjustified basis.[88]

Put another way, surveillance means "watching," but not "potential watching." In a functioning legal system, "potential" is controlled by safeguards that mean the sheer possession of bulk data does not morph seamlessly into watching. The response to the surveillance proportionality concern is, therefore, again one of process, focused on oversight and review. The question posed by both objections, therefore, is whether the *NSA 2017* CSIS dataset regime contains sufficient safeguards.

In the Canadian context, the collection and use of big data by a state agency also raises *Charter* issues. How does section 8 constrain the collection of various pieces of information, none of which individually create a reasonable expectation of privacy, but which when pooled and deciphered using technology may paint an intimate portrait of an individual? How might a court issue a warrant for data collection where there is not an identified target?

---

86 House of Commons, *Government Response to the Report of the Standing Committee on Public Safety and National Security: Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries* (June 2009) (Chair: Garry Breitkreuz), online: <ourcommons.ca/DocumentViewer/en/40-2/SECU/report-3/response-8512-402-123?page=9>.

87 Some scholars argue that mass surveillance is unlawful or unduly violative of democratic values, and as such the law ought not allow for even the collection of data that facilitates such surveillance. See e.g. Christopher Parsons, "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance" (2015) 3:3 Media & Communication 1; Eliza Watt, "The Right to Privacy and the Future of Mass Surveillance" (2017) 21:7 Intl JHR 773.

88 Anderson Report, *supra* note 81 at para 1.9 [emphasis in original].

Can privacy "be preserved in any real way if bytes are cumulated into a single, master database, or chain of linked databases"?[89]

Since section 8 of the *Charter* is a modulated right, protecting against only "unreasonable" searches and seizures, the response to these *Charter* questions is also a process matter: what safeguards does the *NSA 2017* contain that might make "reasonable" any searches and seizures stemming from the collection, retention, and use of CSIS datasets?

C. THE MECHANICS

Addressing these questions requires, therefore, a detailed analysis of the CSIS dataset regime's mechanics.

1. THE TECHNICAL DILEMMAS

As amended by the *NSA 2017*, section 2 of the *CSIS Act* defines a dataset as "a collection of information stored as an electronic record and characterized by a common subject matter."[90] The *CSIS Act* only governs dataset collection if a dataset contains personal information — defined in section 3 of the *Privacy Act* as "information about an identifiable individual"[91] — and "does not directly and immediately relate to activities that represent a threat to the security of Canada."[92] Depending on the circumstances, personal identifying information can be anything from one's ethnicity to a telephone number or one's university alma mater. Importantly, personal (or any other) information that *does* relate to threats to the security of Canada need not meet the standards in the dataset regime — CSIS may *already* retain that information under the terms of section 12, allowing retention of information strictly necessary to the security of Canada.

The acquisition of personal information by CSIS is the reason why the dataset regime is so complex (it alone adds 20 pages to what was originally a 30-page piece of legislation.) This is because collecting this information is likely also to qualify as a search or seizure, thereby triggering section 8 protections. Personal information may often be information in which someone has a "reasonable expectation of privacy," a concept whose sweep included "informational privacy": "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[93] Information attracting constitutional protection includes "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[94]

Since *Hunter v. Southam Inc.*, section 8 of the *Charter* has protected against *unreasonable* invasions of reasonable expectations of privacy.[95] A search is presumptively unreasonable

---

89 Craig Forcese, "The Limits of Reasonableness: The Failures of the Conventional Search and Seizure Paradigm in Information-Rich Environments" (Paper delivered at Privacy Commissioner of Canada Insights on Privacy, 23 June 2011) at 9, online: <ssrn.com/abstract=1945269>.

90 *CSIS Act*, *supra* note 2, s 2.

91 RSC 1985, c P-21.

92 *CSIS Act*, *supra* note 2, s 11.02.

93 *R v Tessling*, 2004 SCC 67 at para 23, citing Alan F Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

94 *R v Plant*, [1993] 3 SCR 281 at 293.

95 [1984] 2 SCR 145.

if not pre-authorized by a neutral and impartial arbiter capable of acting judicially, issuing an authorization on reasonable and probable grounds.[96] Where a search is not pre-authorized by this arbiter, the state nonetheless may prove that a search is reasonable if it is authorized by a reasonable law and the search itself is carried out in a reasonable manner.[97]

Applying these standards to bulk information collection and big data analytics raises two technical challenges. First, using bulk data could trigger section 8 protections twice: once when CSIS initially acquires the data in which a person has a reasonable expectation of privacy, and then again when it searches through data to create an intimate mosaic of useful information about a target of investigation.

Second, obtaining prior authorization to conduct a search or seizure requires a certain degree of understanding about what the state expects to find or obtain. A neutral arbiter (typically a judge) must be able to assess the intrusiveness of the sought-after information, and weigh that against the state's interest in obtaining the information, when determining the reasonableness of the requested search under section 8 of the *Charter*.[98] "In other words, an assessment must be made of the context of each 'particular situation,' and its impact on '*the individual*.'"[99] Realistically, CSIS may not always have the information needed to satisfy this requirement before collecting a dataset. Prior to analysis, it may not have enough understanding about the type of personal information contained within a dataset, or the extent of the state's interest in retaining and using that information.

Imagine, as an example, that a foreign intelligence partner provides CSIS with a list it has compiled of foreigners crossing the border from Syria into Turkey, some of whom are believed to be Canadian. This list would undoubtedly contain the names and personal information of individuals who pose no threat to the security of Canada and, as such, CSIS could not retain the list in its entirety under its section 12 mandate. Furthermore, the collected information about Canadians on the list may or may not be of a nature to trigger section 8 of the *Charter*. Thus, without receiving and reviewing the list, there is no way for CSIS to know the extent of the personal information contained therein, whether that personal information engages section 8 protections, or how useful the list may be for any number of section 12 investigations. Without that information, CSIS could not provide a judge with enough information to engage in the necessary balancing of interests to authorize the dataset collection under section 8.

Moreover, practically speaking, it would also be extraordinarily burdensome and ineffective to require CSIS to obtain prior judicial authorization every time it seeks to query a dataset. Technically, under the *CSIS Act* definition, the Ottawa telephone directory is a dataset; albeit one in which no one has a reasonable expectation of privacy. But in a world

---

96 *Ibid* at 162; *R v Spencer*, 2014 SCC 43 at paras 68–71 (in the criminal law context, there must be reasonable and probable grounds to believe that an offence has been committed and that there is evidence to be found at the place to be searched).

97 *R v Collins*, [1987] 1 SCR 265 [*Collins*].

98 *X (Re)*, 2017 FC 1048 at para 51 ("[b]roadly speaking, a determination of whether a search is unreasonable requires a balancing assessment of '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'").

99 *Ibid* at para 61 [emphasis in original].

of analytics in which intimate (and potentially *Charter*-protected) personal information may emerge from the pooling and linking of otherwise benign information, should CSIS be expected to apply to the Federal Court for an authorization every time an investigation requires it to run a search of a subject of investigation's name or phone number in its databases? Certainly, such a scenario would be operationally infeasible and overly taxing on the resources of the Federal Court.

2. COLLECTING "BUCKETS"

To balance these operational realities against the section 8 implications of bulk data analytics, the CSIS dataset regime employs a series of oversight and review features that vary according to the content of a dataset. Datasets are therefore subdivided by content into three categories (which we sometimes call "buckets"): publicly available, Canadian, or foreign.[100] A Canadian dataset is one that predominantly relates to Canadians or persons within Canada, while a foreign dataset predominantly relates to non-Canadians outside Canada.[101]

To collect any dataset, CSIS must be satisfied that it "is relevant to the performance of its duties and functions" under the *CSIS Act*.[102] Additionally, before acquiring a Canadian dataset, CSIS must be convinced that it falls within a pre-approved class of datasets authorized for collection by the Minister of Public Safety.[103] The Minister's class authorizations are valid for no more than one year and are also subject to approval on a reasonableness standard by the Intelligence Commissioner, a new quasi-judicial oversight body staffed by a retired judge.[104]

3. RETENTION

In the initial 90 days following acquisition, or until an authorization to retain is sought and approved, CSIS cannot use the information in the dataset to derive intelligence, except in exigent circumstances where life, individual safety, or perishable information of significant value to national security is at risk of being lost.[105]

This 90-day window provides time for CSIS to ascertain what information the dataset contains and if that information may be useful to an ongoing investigation, and to prepare its application to present to the Court or the Minister. Accordingly, all CSIS is permitted to do in the first 90 days is delete extraneous, erroneous, or poor quality information; translate, decrypt, and organize the dataset; and apply privacy protections.[106] Furthermore, during the initial collection phase, and for as long as CSIS retains a dataset, it is obligated to delete any information related to a person's mental or physical health in which there is a reasonable expectation of privacy, and information that is subject to solicitor-client privilege.[107] At any

---

100 *CSIS Act*, *supra* note 2, s 11.01.
101 *Ibid*, s 11.07(1).
102 *Ibid*, s 11.05(1).
103 *Ibid*, s 11.03.
104 *Ibid*, s 11.03(3).
105 *Ibid*, s.11.22.
106 *Ibid*, s 11.07(5).
107 *Ibid*, ss 11.1(1)(a)–(b).

time, if a dataset is classified as foreign, any Canadian information found in it must be destroyed, or processed as a separate Canadian dataset.[108]

To retain a Canadian dataset for longer than 90 days, CSIS must obtain the Minister's approval and then obtain judicial authorization from the Federal Court.[109] To retain a foreign dataset beyond the initial 90-day consultation period, CSIS needs the authorization of the Minister, a decision then reviewed on reasonableness grounds by the Intelligence Commissioner.[110] The Court and Minister may only issue an authorization if they are satisfied that the dataset is likely to assist CSIS in the performance of its duties and functions.[111] Both issuing authorities can impose any terms and conditions on the retention and use of a dataset that they consider advisable in the public interest.[112] We can expect that those conditions, like the conditions of classic *CSIS Act* warrants, will be applied to ensure the reasonableness of CSIS's use of a dataset, in light of the intrusiveness of the personal information it contains.

Once retention is authorized by the Federal Court, Canadian datasets may be retained for up to two years. Foreign dataset retention authorizations are valid for a maximum of five years.[113] Publicly available datasets, on the other hand, can be retained indefinitely without authorization, so long as all irrelevant personal information is deleted.

4. QUERYING AND EXPLOITATION

Following retention, the *CSIS Act* defines two types of data analytics that can be performed on datasets: "queries" are specific searches relating to a person or entity within one or more datasets, and "exploitation" means "a computational analysis of one or more datasets for the purpose of obtaining intelligence that would not otherwise be apparent."[114] Querying or exploiting a Canadian or foreign dataset must be *strictly necessary* to CSIS's security intelligence and threat reduction mandates, or required for its foreign intelligence function.[115] Foreign datasets may also be queried or exploited where *strictly necessary* for CSIS's security screening assessment mandate under section 15 of the *CSIS Act*. Any retention of the results of a query or exploitation must be *strictly necessary* to the performance of CSIS's threat intelligence, threat disruption, and security assessment mandates, or *required* to assist CSIS's foreign intelligence mandate.[116]

5. BACKEND SAFEGUARDS

An essential safeguard in the dataset regime is that all Canadian and foreign datasets must be walled off from the rest of CSIS's holdings and are only accessible to a limited number

---

108 *Ibid*, s 11.1(1)(c).
109 *Ibid*, ss 11.12–11.13.
110 *Ibid*, ss 11.17–11.18.
111 *Ibid*, ss 11.13(1), 11.17(1).
112 *Ibid*, ss 11.14(1)(e), 11.17(2)(e).
113 *Ibid*, ss 11.14(2), 11.17(3).
114 *Ibid*, s 2.
115 *Ibid*, s 11.2(2).
116 *Ibid*, s 11.21. Section 11.21(1)(a) does not refer to "strictly necessary," but the cross-reference to section 12 implicitly imposes the classic section 12 "strictly necessary" requirement.

of persons specially designated by the CSIS director.[117] Only after the results of a query or exploitation are found to be fruitful, and the retention of these results is determined to be *strictly necessary*, can a designated person flip the result to the other side of the wall so that it can be used by CSIS officers to further an investigation.[118] If not retained, all results must be destroyed.[119] The Act requires that CSIS record every step of this process, including an analyst's justification for conducting a query and the basis for retaining results.[120] Together, these requirements should prevent CSIS from amassing files of identifiable information about Canadians unless doing so is strictly necessary to advance an investigation of a threat to the security of Canada.

The law also requires periodic and random auditing, and CSIS must provide all auditing reports to NSIRA.[121] Moreover, should NSIRA believe the querying or exploitation of a dataset may not comply with the law, it can refer the matter to the Federal Court.[122] This is a unique feature that gives the back-end review of the dataset regime considerable significance. Findings of NSIRA are non-binding and, as we noted with SIRC's recommendations in the case of ODAC, may be wholly ignored. However, by giving NSIRA what amounts to a line of communication with the Federal Court and giving the Court the jurisdiction to respond to NSIRA's findings and make whatever order it sees fit, the dataset regime is made more robust. Indeed, it makes it more likely a court would consider the system a reasonable law, applied reasonably within the meaning of section 8 of the *Charter*, if information triggering a reasonable expectation of privacy is at issue.[123]

D. ASSESSMENT

1. OVERVIEW

In net, the *NSA 2017* dataset system amounts to a quid pro quo: CSIS's traditional section 12 constraints are loosened to the extent that it may compile a broader haystack of data. But retention of this bulk data (at least for Canadian datasets) requires judicial supervision.[124] This system recognizes that privacy interests extend beyond the point of collection and include retention and use. In so doing, it short-circuits inevitable frontier section 8 *Charter* issues, specifically, questions noted above about whether section 8 attaches to data analytics. As we see it, the *NSA 2017* anticipated and preempted these issues by introducing an independent judicial arbiter who can guide and condition big data analysis — although not to the degree of approving each individual query. Meanwhile, the back-end NSIRA review

---

117 *Ibid*, s 11.24(3).

118 *Ibid*, s 11.21. When read in conjunction with section 11.24(3) this is made clear through the language "[t]he Service may retain the results of the query" rather than the narrow authorization for retention by a designated person.

119 *Ibid*, s 11.21(2).

120 *Ibid*, s 11.24.

121 *Ibid*, s 11.25.

122 *Ibid*, s 27.1.

123 Under *Collins*, *supra* note 97 at 278, for a warrantless search to be lawful, (1) the search must be authorized by law, (2) the law itself must be reasonable, and (3) the search must be carried out in a reasonable manner.

124 The Privacy Commissioner makes (essentially) this same point, and offered no recommendations for changes to the CSIS dataset regime in the *NSA 2017*. See Letter from the Privacy Commissioner of Canada to the Honourable John McKay, MP (5 March 2018) at 12, online: *House of Commons* <ourcommons.ca/Content/Committee/421/SECU/Brief/BR9707885/br-external/OfficeOfThePrivacyCommissionerOfCanada-e.pdf> [Privacy Commissioner Letter].

process is webbed closely into the oversight regime, and can feed it in a manner that will aid and assist judges. This approach demonstrated considerable foresight.

Still, at this writing, we have one lingering doubt about this constitution-proofing of the CSIS dataset regime. And we acknowledge a related concern about how well the oversight and review system can function in a technologically sophisticated environment.

a. Publicly Available Datasets

In relation to the first concern: the Federal Court retention authorization (and the Intelligence Commissioner approval of dataset classes) is limited to "Canadian datasets."[125] Datasets primarily comprising information on foreign individuals outside Canada are processed under a separate regime, in which the Intelligence Commissioner decides the retention issue. Since *Charter* privacy rights are largely geographic in scope, this more relaxed system is probably justifiable. Nonetheless, the third class of datasets comprises personal information "publicly available at the time of collection."[126] Publicly available datasets are not subject to any independent oversight regime.

It matters, therefore, into which of these three "buckets" information is placed. Some information may be publicly available (for example, hacked private information dumped on the Internet or the sort of information at issue in the Cambridge Analytica/Facebook matter)[127] but still raise considerable privacy implications, including possibly under the *Charter*.[128] CSIS has indicated before Parliament that it will not treat hacked information as publicly available.[129] This is, however, a policy decision, not one required by law. Should CSIS adopt an underinclusive policy that steers information in which a Canadian still has a reasonable expectation of privacy into the "publicly available" bucket, the constitutionality of this practice would be suspect and raise the prospect of an ODAC controversy rerun.

The obvious solution would have been to amend the *NSA 2017* to define "publicly available" as excluding "information in which a Canadian or person in Canada retains a reasonable expectation of privacy." This would have had the effect of steering such information into the "Canadian dataset" bucket, with its (more constitutionally robust) oversight system. Parliament declined to make such an amendment despite calls for reform from the Canadian Civil Liberties Association and others.[130] At the very least, therefore, the

---

125 *NSA 2017*, *supra* note 1, s 50.

126 *CSIS Act*, *supra* note 2, s 11.07(1)(a).

127 For a discussion of Cambridge Analytica and Facebook, see House of Commons, *Addressing Digital Privacy Vulnerabilities and Potential Threats to Canada's Democratic Electoral Process: Report of the Standing Committee on Access to Information, Privacy and Ethics* (June 2018) (Chair: Bob Zimmer), online: <ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9932875/ethirp16/ethirp16-e.pdf>.

128 As an illustration of how "publicly available" information may still be clothed in privacy expectations, see Office of the Privacy Commissioner of Canada, *Complaints under the Personal Information Protection and Electronic Documents Act (the "Act" or "PIPEDA") against Profile Technology Ltd.*, PIPEDA Report of Findings #2018-002 (Ottawa: OPC, 2018), online: <priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2018/pipeda-2018-002/>.

129 House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 42-1, No 97 (13 February 2018) at 1220 (Tricia Geddes).

130 Canadian Civil Liberties Association, "Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, *An Act respecting national security matters*" (Toronto: CCLA, 2018), online: <ccla.org/cclanewsite/wp-content/uploads/2018/01/2018-01-17-Written-submissions-to-SECU-re-C-59.pdf>. Notably, the Privacy Commissioner of Canada raised the definitional issue with respect to the phrase "publicly available information" and recommended an amendment in the proposed

Minister of Public Safety should issue a ministerial direction with the same effect — and ensure that this direction and any of its successors are public to create confidence in otherwise opaque internal procedures within CSIS.

b. Algorithmic Bias

A more difficult question is whether a system of big data exploitation likely to be built around machine learning can be effectively overseen and reviewed. There is now considerable discussion of "algorithmic bias" — that is, machine-based forms of querying and exploitation of data that embed discriminatory presuppositions.[131] Part of this phenomenon reflects the poor quality of the information on which data analytics may be based — "garbage in" may equal "garbage out." This itself is not a new problem for intelligence practitioners, and assessing the quality and reliability of the data in a dataset will not be a novel problem within CSIS. More insidious may be the implications of algorithms built on machine learning whose workings are not fully understood by users, or are built by biased architects. The algorithmic models themselves may create biased outcomes. In predictive policing, for example, "[u]sing models of risk as a basis for police decision-making means that those already subject to police attention will become increasingly profiled. More data on their offending will be uncovered. The focus on them will be intensified, leading to more offending identified — and so the cycle continues."[132] Put another way, if one searches only under the street light, what one finds will reaffirm algorithmic preference for searching places under the street light.

Countering this self-affirming bias — as deleterious to effective security as it is to civil rights — will require considerable technical competency in CSIS. Assessing its existence will require equivalent competence among oversight and review bodies. Whether the Federal Court, the Intelligence Commissioner, and the NSIRA can marshal this capacity, and truly understand what it is they authorize and review, remains to be seen. At the very least, it seems likely the Federal Court will need to employ "technical" amici curiae, and not just the barristers who traditionally perform this role. The Intelligence Commissioner and NSIRA, for their parts, will need researchers with the skills required to audit big data methodologies. It remains to be seen how nimble the Federal Court, the Intelligence Commissioner, NSIRA, and CSIS itself will be in responding to the problem of algorithmic bias.

V. CONCLUSION

The *CSIS Act* was designed for an analog period, in which CSIS's mandate was limited to the collection of information, and the provision of intelligence, in a relatively data-poor world. During that period, the Supreme Court, SIRC, and the Air India Commission all

---

Communications Security Establishment Act, which was ultimately supported by Parliament. The Commissioner did not, however, suggest an amendment to this definition in the *CSIS Act*. See Privacy Commissioner Letter, *supra* note 124 at 10–11.

131 See e.g. Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018); Joni R Jackson, "Algorithmic Bias" (2018) 15:4 J Leadership, Accountability & Ethics 55; Sandra G Mayson, "Bias In, Bias Out" (2019) 128:8 Yale LJ 2218.

132 Mike Rowe, "AI Profiling: The Social and Moral Hazards of 'Predictive' Policing," *The Conversation* (7 March 2018), online: <theconversation.com/ai-profiling-the-social-and-moral-hazards-of-predictive-policing-92960>.

condemned CSIS's seemingly laudable practice of destroying original operational information, pointing to the due process and evidentiary implications of this policy. CSIS was, in other words, undershooting in its information retention policies.

More recently, CSIS has struggled to adjust to a new information-rich world — one with rich sources of intelligence derived from third-party metadata. Here, CSIS overshot the mark, retaining too much and drawing the ire of the Federal Court in 2016. With that decision, the lawfulness of CSIS's data analytics programs were cast in doubt, and CSIS no longer was an intelligence service able to operate in the modern world of big data analytics.

The challenge then became finding a constitutionally compliant, civil-rights-respecting but security-useful solution. The *NSA 2017* attempts to strike this balance by superimposing an independent Intelligence Commissioner and, for Canadian datasets, a judge to perform oversight roles. At the same time, it creates an enhanced review body, the NSIRA, to perform back-end review.

We are right to be wary of such a regime since it depends on close adherence to a complicated set of checks and balances. This complicated system means datasets cannot, in fairness, be equated with "mass surveillance." Still, satisfying core civil liberties issues will depend, we believe, on the attentiveness of CSIS, its oversight bodies, and the NSIRA to the implications of algorithmic bias. Further, we anticipate that the adjudication of the regime's constitutionality will turn on how widely CSIS and the Minister set the guard rails. For instance, how broadly "classes" of Canadian datasets are defined, the number of designated employees with access to the datasets, the robustness of the auditing and spot checks carried out by CSIS, and how narrowly CSIS interprets the thresholds of "relevance," "likely to assist," and "strictly necessary" would likely all factor into a court's assessment of the regime's constitutionality. Any attempt to stretch the parameters of the legislation in the same way CSIS overreached in the ODAC Decision would be the quickest path to disaster.

It is also worth noting that the structure of the authorization scheme could open the door to some rather troubling litigation for CSIS. For instance, if the Minister or the Intelligence Commissioner refused to authorize the retention of a foreign dataset, might CSIS seek a judicial review of that decision at the Federal Court? Moreover, what remedies can the Federal Court order if they agree with NSIRA and find that CSIS conducted an unlawful query? Could the Court order a personal remedy if it determines that CSIS violated a Canadian's right to privacy, and, if so, what would that look like? These questions remain theoretical at this writing.

In conclusion, it is certainly possible to imagine even more safeguards and precautions in the dataset system. Still, we accept the policy justification for the dataset regime. And we accept the checks and balances imposed cannot become so burdensome that intelligence services are left to obtain, essentially, a warrant to obtain information justifying the issuance of a warrant. Put another way, the *NSA 2017* seeks balance. In our view (and subject to the doubts we have flagged), it succeeds in giving new powers, while also imposing significant new responsibilities.

[*this page is intentionally blank*]