David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

Reconciling Privacy with National Security

Submissions
to the Department of Public Safety Canada
and to the Department of Justice

■

Regarding Warrantless Access
to Basic Subscriber Information

Prepared by the David Asper Centre's Working Group on Privacy and National Security

15 December 2016
Toronto, Canada

Working Group Editors
Carolyn Mouland, Lauren Pinder, Geneviève Ryan, Sarah Teich

Working Group Contributors
Stuart Agnew, Rachel Chan, Patrick Enright, Abigail Herrington, Albert Kwan, Patrick Liao, Carolyn Mouland, Dylan Murray, Nicole Nazareth, Lauren Pinder, Colin Romano, Geneviève Ryan, Kennedy Simpson, Daniel Sisgoreo, Emily Stewart, Sarah Strban, Sarah Teich, Glen Tucker, Mark Wolfe, Alexia Yang

A special thanks to Cheryl Milne, Tal Schreier, Kent Roach and Lisa Austin for their helpful comments and guidance throughout the research and writing process.

Reconciling Privacy with National Security

Submissions to the Department of Public Safety Canada and the Department of Justice
Regarding Warrantless Access to Basic Subscriber Information

About the David Asper Centre for Constitutional Rights

The David Asper Centre for Constitutional Rights is a centre within the University of Toronto, Faculty of Law devoted to advocacy, research and education in the area of constitutional rights in Canada. The Centre houses a unique legal clinic that brings together students, faculty and members of the legal profession to work on significant constitutional cases. Through the establishment of the Centre, the University of Toronto joins a small group of international law schools that play an active role in constitutional debates of the day. It is the only Canadian Centre in existence that attempts to bring constitutional law research, policy, advocacy and teaching together under one roof. The Centre aims to play vital role in articulating Canada's constitutional vision to the broader world. The Centre was established through a generous gift to the law school from U of T law alumnus David Asper (LLM '07).

About the David Asper Centre's Working Group on Privacy and National Security

We are a group of 20 law students at the University of Toronto Faculty of Law united by our interests in national security and privacy law. Our mandate is two-fold: first, to examine the privacy implications of Bill C-51 and related national security legislation; and second, to advocate for enhanced accountability when personal information is acquired, used, and retained for national security.

Contents

Summary of Recommendations

- Any modernization of the current system of search warrants (to better serve efficiency, etc.), must continue to protect the fundamental rights and freedoms enshrined in the *Charter*, including the right to be free from unreasonable search and seizure under section 8
- An expedited, digital approach to warrants would enable law enforcement to act quickly, while better adhering to the constitutional requirements of section 8
- The *Green Paper* proposals do not adhere to the constitutional requirements of section 8 as they constitute unacceptable diminutions of our *Charter* rights.
    a. The *Green Paper's* proposed standard of reasonable suspicion (for CSIS to obtain lawful access to subscriber information and for obtaining warrants) is an inappropriately low threshold for the protection of subscriber information
    b. The standard that should be applied is that of "reasonable and probable grounds"
- To justify legislative changes that impact constitutionally-protected privacy rights, there should be evidence that these changes are warranted
- Parliament should take this review as an opportunity to address limitations in the current scheme, namely: the need for consistency, the fallibility of warrants, and the need for post-collection accountability and safeguards especially with respect to information-sharing which itself is subject to section 8 protections
    a. Any new regime should include safeguards for information sharing that include a record-keeping requirement, a reporting requirement to an independent oversight body, and notice of the disclosure to the person whose information was accessed if issuing notice is not, in the circumstances, injurious to national security
- Federal law needs to clearly prohibit the voluntary disclosure of subscriber information by telecommunications companies
    a. Following the modernized, digital approach to section 8, warrants should also be required for telecommunications companies to disclose personal information, including subscriber information
    b. Requests and disclosures of such information should be promptly and accurately recorded and reported to an oversight body, with notice of the disclosure to the person whose information was accessed if issuing notice is not, in the circumstances, injurious to national security
- Parliament should develop an approach to metadata and national security that reflects on the strengths and weakness of other jurisdictions in order to adopt the best approach possible. It should do so in four areas:
    a. If Parliament chooses to enact a data retention scheme, it must proportionally balance the interests that law enforcement and security agencies have in preservation of data with the individual and societal interest in privacy protection including Charter protections
    b. All legislation should adhere to the requirement of judicial authorization to access individual's information on the standard of reasonable and probable grounds
    c. Parliament should limit information sharing between agencies under SCISA through clear, reasonable standards and robust control mechanisms
    d. Parliament should implement a review system with a mandate as broad as the collaboration between the security agencies it oversees

Introduction

The intersection of technology and national security is rapidly changing how we see the world and how we behave and communicate within it. While Canada has evolved post-Confederation and since the entrenchment of the *Charter of Rights and Freedoms* (the *Charter*)[1], what remains *unchanged* is the government's mandate "to safeguard the people, institutions and values of Canada".[2] Our expectation is for the government to protect us from threats against us, our institutions and our values, but without sacrificing the fundamental rights and freedoms guaranteed to us all under the *Charter*.

The primary subject matter of this submission is warrantless access to basic subscriber information for national security purposes. Through this lens, we also raise broader concerns for accountability and transparency. Our *Charter* rights are endangered by the implementation of Bill C-51 and the current *Green Paper* proposals to facilitate access to basic subscriber information. We are especially alarmed by the *Green Paper*'1s proposal to grant administrative access to basic subscriber information without prior judicial authorization. Search warrants provide protection against unreasonable search and seizure. In the criminal law context, the Supreme Court of Canada has already decided that warrantless access to subscriber information constitutes an infringement of section 8. Nevertheless, as articulated in *Hunter v Southam Inc*, warrants *per se* are not a constitutional precondition. Modernizing the current system is acceptable. Improving it is necessary, in fact – but we urge the government to modernize and improve access to information in a manner that respects the constitutional parameters of section 8 and fosters the spirit of the *Charter*.

This submission begins with the constitutional framework for search warrants (Part I). Section 8 of the *Charter* forms the backdrop for our submission highlighting the flexibility (and the boundaries of that flexibility) available to Parliament in refashioning the search warrant regime. Part II then builds from the constitutional context to address the *Green Paper* proposals specifically. We believe the current proposals would effectively overrule *R v Spencer* in violation of our guaranteed privacy rights. Before concluding Part II, we analyze the national security context to identify a troubling lack of evidence to support the *Green Paper's* proposed lower threshold for authorization and easier administrative access to subscriber information. Part III encourages Parliament to take this opportunity to address several limitations in the current scheme: inconsistent standards across law enforcement agencies and data regimes, the fallibility of warrants, and the national security (post-collection) accountability gap. Lastly, Part IV provides insight on implementing our recommendations by reviewing best and worst practices from other jurisdictions. In sum, the theme of our submission is that our constitutional right to privacy and the government's mandate to protect us are compatible, reconcilable goals that are attainable when basic subscriber information is sought for national security purposes.

[1] *Canadian Charter of Rights and Freedoms*, Part 1 of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), c 11.
[2] Canada, Public Safety Canada, Our Security, Our Rights: National Security Green Paper 2016: Background Document, (Ottawa: 2016) at p 6 [Green Paper].

Part I: Background Information: Warrants and their Constitutional Protection

Warrants as Justified Law Enforcement

Before delving into our critique of the *Green Paper* proposals, we must clarify the role of a search warrant. A search warrant does more than symbolize the authority of the officer to act for the state – it is *proof* of *justified* authority to enforce the law.

In the law enforcement context, warrants serve two instrumental purposes: they are a mechanism for gathering evidence (seizing) and a method of investigation (searching). Warrants are important because they enable law enforcement "not only to seize evidence but also to ascertain that it exists, and even sometimes that the crime was in fact committed and by whom. Seizure makes it possible to preserve the evidence."[3] But warrants are more than a mere authorization for search and seizure. A warrant signals not only the exercise of authority, but that there are good justificatory reasons for the intrusion it permits, and that it is the state who must be ultimately responsible for that intrusion.

The Purpose (and Requirements) of Section 8: Preventing Unjustified Searches

Section 8 of the *Charter* guarantees the right "to be secure against unreasonable search or seizure." A search warrant signals that there are good justificatory reasons for the intrusion it permits, thus guarding against unjustified searches, as per section 8 of the *Charter.* The landmark case of *Hunter v Southam Inc* makes this clear. In *Hunter*, Justice Dickson (as he then was) pronounced that the purpose of section 8 is to "protect individuals from unjustified state intrusions upon their privacy".[4] This inherent justificatory aspect within section 8 "requires 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."[5]

Hunter is also indispensable for setting the constitutional requirements of section 8 of the *Charter* (outlined below), and for fortifying our Constitution's prospective and purposive capacity for "growth and development over time to meet new social, political and historical realities often unimagined by its framers."[6] The constitutional requirements of section 8, together with the Constitution's purposive capacity for growth, suggest that while we can make changes to the current system of search warrants (to better serve efficiency, etc.), we must continue to protect the fundamental rights and freedoms enshrined in the *Charter*, including the right to be secure against unreasonable search or seizure. The *Charter* jurisprudence has indeed grown to recognize that section 8 also protects the sharing of information once acquired, both domestically and internationally.[7]

---

[3] *Descôteaux v Mierzwinski*, [1982] 1 SCR 860 at p 891; *Canadian Oxy Chemicals Ltd. V Canada (Attorney General),* [1999] SCR 743 at paras 20-22.
[4] [1984] 2 SCR 145 at p 160 [*Hunter*].
[5] *Ibid* at p 155.
[6] *Ibid*.
[7] *R v Quesnelle,* 2014 SCC 46; *Wakeling v United States of America, 2014 SCC 72* [*Wakeling*].

Constitutional Requirements of Section 8

1. Prior Authorization: *Hunter* established that a warrant *per se*, is not a constitutional precondition. What is required, however, is a prior authorization in order "for the conflicting interests of the state and the individual to be assessed, so that the individual's right to privacy will be breached only where the appropriate standard has been met, and the interests of the state are thus demonstrably superior." Prior authorization is almost always required when a person holds a reasonable expectation of privacy in the information sought – the exceptions to judicial authorization happen only with minimally invasive measures that do not go to a person's 'biographical core' (for example, dog sniff searches). This is because privacy interests are personal rights held by people.

2. Independent and Impartial Arbiter: For this prior authorization to be meaningful and effective, it can only be granted by an independent and impartial party. Although this adjudicative role has been traditionally performed by a judge (even at common law before the *Charter*), *Hunter* is clear that the arbiter need not be a judge. The arbiter of the decision to preauthorize must only be detached and neutral from the investigatory agency. In keeping with this requirement, the Federal Court, which has designated judges with national security expertise, might be a logical choice of arbiter to handle national security warrants.

3. Reasonable and Probable Grounds: Under section 8 of the *Charter*, the individual has a protected right to a "reasonable expectation of privacy" which is determined based on a number of factors, including the "totality of the circumstances" and whether or not the information is part of an individual's "biographical core". This means that the appropriate standard for the justification can vary according to the nature of each competing interest. However, an officer must always prove there is a nexus between the subject matter of the search, where the evidence is located, and that an offence has been or is being committed. Simply put, a warrant is given where the court is satisfied that it *will* produce the evidence sought by police – not merely that it 'may' or 'could' produce such evidence.

Looking to the constitutional requirements of section 8, it becomes evident that in three key aspects, *Hunter* envisions a level of creativity and flexibility for safeguarding the individual's privacy interests, but tailored to the context where the information is sought. The constitutional requirements outlined in *Hunter* make it clear that a warrant *per se* is not a constitutional requirement; that the arbiter need not be a judge; and that the appropriate standard for the justification can vary according to the nature of the competing interests.

These three nuances of the constitutional parameters of section 8 *Hunter* are important because they provide the means to modernize the traditional warrant procedure in a way that overcomes the obstacles of time repeatedly cited by our national security agencies, while also protecting the privacy rights of individuals.

One way to creatively modernize the current system might be digitization. An expedited, digital approach to warrants might enable law enforcement to act quickly, but without circumventing the constitutional requirements outlined in *Hunter.* This might be a natural extension of the "telewarrant" – which expedites the authorization process in urgent cases. As an alternative to the questionable Green Paper proposals, **we suggest that a system of e-warrants, submitted via a secure online system to impartial arbiters with national security expertise might be one route to modernized, efficient access.**

It is also important to note that the search and seizure protections of section 8 do not end when police obtain a warrant. State officials, including law enforcement officials, do not have the right to do anything they wish with lawfully obtained information. As the Supreme Court of Canada stated in *R v Mills*:

> "*Privacy is not an all or nothing right. It does not follow from the fact that the Crown has possession of the records that any reasonable expectation of privacy disappears. Privacy interests in modern society include the reasonable expectation that private information will remain confidential to the persons to whom and restricted to the purposes for which it was divulged.*"[8]

This growth of section 8 is not stunted by information-sharing legislation that permits sharing between Canadian officials and departments, nor sharing with foreign states. The Supreme Court affirmed in *R. v. Quesnelle* that protection around subsequent uses is not restricted to "trust-like, confidential, or therapeutic relationships."[9] Disclosures outside "the purpose for which it was obtained or a consistent purpose" violate a reasonable expectation of privacy.[10] Sharing of information with foreign states for law enforcement purposes can also trigger a residual expectation of privacy and attract *Charter* scrutiny.[11]

Part II: The *Green Paper* Proposals: Unacceptable Diminutions of our *Charter* Rights

The *Green Paper* suggests lower evidentiary requirements for CSIS to obtain lawful access to information and for obtaining warrants. Under Bill C-51, the threshold for initiating an investigation is low – CSIS need only demonstrate that it has "reasonable grounds to suspect that an activity is a threat."[12] It also alleges that Court rulings in cases like *Spencer* create difficulty in obtaining "timely and effective access" to

[8] [1999] 3 SCR 668 at para 108 [*Mills*].
[9] *Quesnelle, supra* note 7 at para 27.
[10] *Ibid* at paras 40-41.
[11] *Wakeling, supra* note 7.
[12] Canada, Public Safety Canada, Our Security, Our Rights: National Security Green Paper 2016: Consultation Document (Ottawa: 2016) at p 11 [Consultation Paper]. See also *Canadian Security Intelligence Service Act*, RSC 1985, c C-23, s 12(1) (*CSIS Act*) which reads:

"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." (emphasis added)

subscriber information. Most troubling is the manner in which the *Green Paper* describes the warrant process as being "disproportionate when the only information investigators are seeking is BSI [basic subscriber information], even if the requirements are proportionate in other situations involving greater privacy intrusions."[13] The *Green Paper* specifically mentions the difficulty of meeting these requirements at the outset of an investigation when it may not have the requisite supporting information it needs to obtain a warrant.[14] This suggests a desire for legislation allowing access on the 'reasonable suspicion' standard.

This reasonable suspicion standard has been defined as requiring an officer to show only that they have objective reasons to believe there is a *possibility* that a crime has been committed.[15] Whether given facts give rise to a reasonable suspicion is assessed on the basis of common sense, flexibility, and practical every day experience, seen through the eyes of the officer's knowledge, training and experience.[16] The problem is: on the reasonable suspicion standard, which need only point to the *possibility* of a crime, the risk of false positives is significantly increased. It is for these reasons that the standard of reasonable suspicion was, until Bill C-51, only applied to situations that entailed a low expectation of privacy and minimally intrusive searches, such as dog-sniffs and border searches.[17]

The Supreme Court of Canada has *already* addressed this issue and determined that there can be a high expectation of privacy [18] in subscriber information – especially when that information is connected to specific internet activity carried out under an anonymous IP address. This high expectation of privacy grounded the conclusion that warrantless access to subscriber information violates section 8 of the *Charter.* Given the highly revelatory nature of subscriber information and the risk of false positives described above, lowering the standard to obtain subscriber information runs counter to the spirit of section 8, which aims to prevent unlawful searches.

This conclusion is also bolstered by the Supreme Court's conclusion that *subscriber information can carry such a high expectation of privacy* that private contracts permitting disclosure do not automatically obviate the need for a search warrant. Legislation that effectively accomplishes the same prohibited result as the private contracts at issue in *Spencer* – namely, disclosure of private information tied to an individual's 'biographical core' without sufficient grounds or lawful authority to request it – is vulnerable to a *Charter* challenge.

It should be noted that the *Spencer* decision allows for an "exigent circumstances" exception in which police can conduct warrantless searches where warrants would otherwise be required. In the context of a national security threat, where harm to the public is imminent, this exception would apply.

---

[13] Green Paper, *supra* note 2 at p 58 (emphasis added).
[14] *Ibid*.
[15] *R v Chehil*, 2013 SCC 49 at para 27.
[16] James A Fontana and David Keeshan, *The Law of Search & Seizure in Canada, 9th ed* (Markham: LexisNexis Canada, 2015) at p 994.
[17] *R v Brown*, 2008 SCC 18; *R v Monney*, [1999] 1 SCR 652.
[18] *R. v. Spencer,* 2014 SCC 43, [2014] S.C.R. 212

Beyond the legal framework, the public voice on this issue is resoundingly clear. A survey prompted by the *Green Paper* probed the opinions of 2,500 Canadians on digital privacy and law enforcement.[19] The greatest consensus was in opposing warrantless access to subscriber information. A mere 35% would support internal authorization by a supervisor or prosecutor. 78% of Canadians want judicial approval before law enforcement can request subscriber information from telecommunications companies. Although the study did not distinguish between RCMP and CSIS, given the capacity for information sharing between these agencies, **we believe that the same standard of judicial approval should apply to both RCMP and CSIS to ensure consistent protection of our digital privacy.**

In addition, as Part II below will show, our review of available data did not yield any evidence to support the assertion that national security is a unique context that would justify easier access to these warrants – and therefore justifying a departure from the *Spencer* precedent. This suggests that when it comes to the national security context, a lowered standard is not only potentially unconstitutional – it may also be unnecessary. For these reasons, elaborated on below, the standard of reasonable suspicion is an inappropriately low threshold for the protection of subscriber information, and the Green Paper proposals recommending this lower standard constitute unacceptable diminutions of our Charter rights. **We therefore reiterate that the appropriate standard to be applied is that of "reasonable and probable grounds."**

The High Expectation of Privacy in Subscriber Information

The nature of privacy interests protected by section 8 has been explored in three decades of *Charter* litigation following *Hunter*. As a personal right attaching to people and not property,[20] the protection of personal information varies according to our reasonable expectation of privacy in that information. In essence, to qualify for protection under section 8 of the *Charter,* you must have an *expectation of privacy*, and that expectation must have been objectively reasonable. This aligns with the stated purpose of informational privacy: to "protect a biographical core of personal information which individuals … would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[21]

R v Plant further emphasized the revelatory potential of information. What grounds a reasonable expectation of privacy is not just information that *itself* reveals details about an individual's lifestyles – but information that may ground detailed inferences about that individual. *R v Plant's* conception of informational privacy was endorsed by the Supreme Court of Canada in *R v Spencer*, enabling it to hold that there is a high expectation of privacy in subscriber information. In fact, the Court in *Spencer* expanded on the understanding of informational privacy by recognizing that a reasonable expectation of privacy includes the protection of

[19] Dave Seglins, Robert Cribb and Chelsea Gomez, "Canadians want judicial oversight of any new digital snooping powers for police: Poll" (17 November 2016) *CBC News,* <online: http://www.cbc.ca/news/investigates/police-power-privacy-poll-1.3854186>
[20] *R v Plant*, [1993] 3 SCR 281, at p 293 [*Plant*]; *Schreiber v Canada (Attorney General*), [1998] 1 SCR 841 at para 19.
[21] *Plant* at p 293.

anonymity – that is, the right not to be identified when engaging in anonymous activity in a public space (for example, when posting in a public forum online).

Similar to the arguments currently espoused in the *Green Paper*, the Crown in *Spencer* urged the Court to view subscriber information as simply "a name, address and telephone number matching a publicly available IP address."[22] The result – *rejected by the Court* – would have been subjecting subscriber information to minimally restrictive investigative safeguards. This reading views the information at issue out of context – without reference to the inferences that may be drawn about an individual once that information has been disclosed. Although at first glance, subscriber information does resemble phone book information, in actuality, it reveals a great deal about an individual. A study by the Office of the Privacy Commissioner of Canada (OPC) to discern the revelatory power of subscriber information is illustrative of this point. The OPC found that subscriber information paired with an IP address revealed a detailed profile of an individual's online presence, including information about registered services, personal interests, organizational affiliations, and geographical location.[23]

For example, the OPC study included profiling of an anonymous Wikipedia contributor. The starting point of the profile was the IP address of the computer used to access Wikipedia, which is logged by the website when the edit is made. Based on that single IP address, the OPC could determine that the individual had edited hundreds of pages on North American television shows to a level that gave away the user's "extensive and specific" interests. The user had also edited numerous history pages, participated in a discussion board about a particular television channel, and "[v]isited a site devoted to sexual preferences following an online search for a specific type of person."[24]

That subscriber information carries a high expectation of privacy should not be contentious. The expectation of privacy in subscriber information is confirmed by the Supreme Court in *Spencer*, supported by the OPC, and the opinions of Canadians. While it is true that the Court's finding in *Spencer* was context-dependent, in the sense that it was subscriber information in the context of a criminal investigation for child pornography, rather than subscriber information as a category that had a high expectation of privacy, we caution against a categorical lowering of the threshold by legislative means. The OPC study highlights how subscriber information in the context of online services and activity can be extremely revelatory. It hardly stretches belief to suggest that subscriber information in the general digital contexts will almost inevitably carry the same high expectation of privacy as was found in *Spencer*.

Moreover, this high expectation of privacy should not be dependent on physical location or device – and again, this should not be contentious. There is no meaningful distinction between accessing the internet from a computer, cellphone or tablet. Likewise, there is no meaningful distinction between accessing the internet from a physical public space, or a physical private space. As the court stated in *Spencer*, "Internet users do not expect their online anonymity to cease when they access the Internet outside their homes, via

[22] *Ibid* at para 24.
[23] OPC, *What an IP Address can reveal about you*, at pp 5-6. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/ip_201305/
[24] *Ibid*.

smartphones, or portable devices."[25] This is further supported by the Court's observation in *Spencer* that the high expectation of privacy was not diminished by the agreements signed with service providers. Although many service contracts include terms indicating an individual's consent to disclosure of their subscriber information in the context of a criminal investigation – the Court in *Spencer* found no negative effect on the reasonable expectation of privacy, because warrantless requests by police do not automatically "trigger an obligation [on the service provider] to disclose personal information".[26] Though the decision in *Spencer* turned on the fact that the contractual provisions, in combination with existing legislation were "confusing and equivocal in terms of their impact on a user's reasonable expectation of privacy,"[27] the overriding message was that an individual should have a *clear sense* of when and why their subscriber information may be handed over to state officials without their consent.

In effect, the lower standard proposed in the *Green Paper* would statutorily authorize the very conduct found to infringe section 8 in *Spencer*. Consequently, this proposed law would only be constitutional if it were found to be reasonable within the meaning of section 8 and then demonstrably justified in a free a democratic society, under s 1 of the *Charter*. It is unlikely that this proposed law would pass the s 1 justification test. While the broad objective of warrantless access (the curtailment of terrorism and other criminal activities) is indeed pressing and substantial, lowering the threshold of a reasonable search and seizure is not minimally impairing. By ordinary statute, the lower threshold would reduce an individual's reasonable expectation of privacy in their subscriber information and online activities, circumscribing section 8 rights. In an increasingly digital world, such a reduction is arguably overbroad, when there are ways to adapt the warrant regime to be more focused and efficient.

National Security Does Not Necessitate Special Treatment

The *Green Paper* argues that the *Spencer* decision and the absence of clear laws governing lawful access to subscriber information make it difficult for state officials to obtain that information in a timely and effective manner. The *Green Paper* discusses a number of alternative approaches, but overall shows a preference for placing lawful access authorizations in the national security context in the control of law enforcement agencies rather than with the courts.[28] In this way, the *Green Paper* proposes less stringent standards for governmental agencies to obtain warrants for subscriber information in cases of national security. The rationale behind the *Green Paper*'s approach to accessing subscriber information is that national security is unique, and that obtaining warrants more quickly and easily is necessary to prevent acts of terrorism. Our review of a number of incidents of terrorism in Canada did not find any evidence to support the assertion that national security is a unique context requiring streamlined access to search warrants.

To determine whether streamlined access to warrants is, in fact, essential to combatting terrorism, we documented and analyzed all the Canadian terrorist incidents from 1990 to present day recorded on the Global

[25] *Spencer, supra* note 18 at para 37.
[26] *Ibid* at para 62.
[27] *Ibid* at para 60.
[28] Green Paper*, supra* note 2 at p 18-19.

Terrorism Database (GTD). The GTD is a comprehensive database outlining the details of both foiled and successfully executed terrorist plots[29]. This analysis sought to find evidence about the role that warrants play in combatting terrorism in Canada. Such evidence relevant to our review might have included:

1. *Instances where search warrants were obtained and successfully used to prevent a terrorist plot*. Such evidence might suggest that existing regulations for warrants to obtain subscriber information are not hindering the prevention of acts of terrorism. Consequently, this might call into question whether less stringent standards to obtain warrants at the expense of Canadian privacy rights are justified.
2. *Instances where online activity revealed a terrorist threat but warrants could not be obtained to prevent the attack from occurring*. Such evidence might suggest that the existing standards to obtain warrants for subscriber information are hindering the prevention of terrorism. Such evidence might provide support for the notion that less stringent standards to obtain warrants are necessary to combat terror.

We expected to find several cases where subscriber information was key to the success or failure of terrorist plots. Surprisingly, we did not find any such cases from 1990 to present day.[30] Not only were we unable to find any incidents where a search warrant led to the prevention of a terrorist plot – we were also unable to find any incidents where the failure to acquire a search warrant led to the successful execution of a terrorist attack. In other words: Our systematic investigation did not yield any evidence to support the assertion that national security is a unique context that requires easier access to search warrants.

There is the possibility that such evidence exists as classified information – but, even if this information does exist and Parliament has access to it during its deliberations, the fact that it is not publicly accessible is itself highly problematic. The lack of transparency from the absence of this information will reduce public confidence in the final decision. **In order to justify legislative changes that impact constitutionally-protected privacy rights, there should be publically-available evidence that these changes are warranted.**

Part III: Status Quo Warrants Not Enough: The Need for Consistency and Accountability

From the discussion and evidence presented above it is clear that Parliament should be wary of streamlining access to search warrants in the national security context. Moreover, Parliament should take this opportunity to address limitations in the current scheme. Although there are many limitations, this submission will focus on the inconsistency of standards, the fallibility of warrants, and the national security accountability gap.

[29] It is worth noting that the GTD is limited, as it does not include incidents that have occurred within the last year. We addressed this limitation by conducting a comprehensive open-source search for recent Canadian terrorist incidents.
[30] Since we found no relevant evidence on the GTD, we examined media reports on each Canadian terrorist incident listed – to ensure that we caught all publically available information regarding the role of subscriber information, and to ensure that the lack of information was not a failing of the GTD. No additional information was found.

The Need for Consistency

The decision in *Spencer* is not enough on its own to protect our section 8 informational privacy rights. Because *Spencer* was only about internet service providers and subscriber information, it has not been automatically applied to other, similarly revelatory data – such as cell phone subscriber information and metadata. Adding to the complexity, CSIS and the RCMP have differing standards for lawful access to metadata which, combined with the information-sharing regime under Bill C-51, allows CSIS to enlist the RCMP in circumventing restrictions on their investigatory powers and also defeats the ruling in *Spencer*. As a result, **we recommend that the law provide a consistent standard for the sharing of personal information and data across all law enforcement agencies on a standard of both relevant and necessary. We also recommend the development of consistent standards for the retention and destruction of that information once it is no longer relevant and necessary.**

CSIS is required to adhere to a standard of 'reasonable and proportionate' measures under its threat disruption mandate to obtain a warrant for search and seizure of information,[31] while the RCMP can obtain the same metadata on a lower standard of "reasonable suspicion", making the level of protection afforded to the individual contingent on the enforcement agency. This differential protection is not only unprincipled and anomalous, but information sharing practices based on the low threshold of "relevance" mean the RCMP can provide to CSIS indirectly what CSIS could not collect itself directly. As Professors Kent Roach and Craig Forcese have cautioned, these inconsistent legal standards can lead to backdoor information sharing, which is especially concerning in light of the different degree of independent review for each body.[32]

The lawful access regime governing metadata under subsections 487.014 – 487.017 of the *Criminal Code* (enacted recently, in 2014) also fails to protect section 8 privacy rights. In a recent case involving the Edmonton Police Service (EPS) it was discovered that law enforcement officers improperly characterized cellphone subscriber information as metadata (i.e., "transmission or tracking data" under the terminology of the *Criminal Code*). The EPS had claimed that a subscriber's identity (i.e. name and address) was metadata. Had the application for a preservation and production order succeeded, police would have been granted authority to find out the subscriber's name and identity on the lower standard of reasonable suspicion, in clear circumvention of the law established by *Spencer*.[33]

While the Alberta Provincial Court in that case concluded that the name and address of cellphone subscribers cannot be accessed through the metadata regime of the *Criminal Code,* the case highlights another problem: the unclear language suggesting that communications service providers can voluntarily disclose

[31] *CSIS Act, supra* note 12, *s 21.1 (3)* allows a judge who is satisfied that the facts relied on justify belief on reasonable grounds that the warrant is required and that the proposed measures are reasonable and proportionate in the circumstances may issue a warrant:

"(a) to enter any place or open or obtain access to any thing;

(b) to search for, remove or return, or examine, takes extracts from or make copies of or record in any other manner the information, record, document or thing."

[32] Craig Forcese and Kent Roach, *False Security: The Radicalization of Canada Anti-Terrorism*, (Toronto: Irwin Law, 2015) at 128-129. [*False Security*]

[33] *Re Subscriber Information,* 2015 ABPC 178.

information under section 487.0195 of the *Criminal Code.* As Judge Henderson observed, "The Court cannot dictate how a telecommunications company will conduct itself in relation to voluntary disclosure."[34] Yet section 487.0195 specifies that no warrant is required for voluntary disclosure of data that "the person is not prohibited by law from disclosing."[35] It is also unclear what "law" s 487.0195 refers to. **We propose that federal law needs to clearly prohibit the voluntary disclosure of subscriber information by telecommunications companies.**

Rather than leave it to the courts to confirm whether or not accessing subscriber information requires a warrant for different services – for example, internet services in *Spencer* and cellular services in *Re Subscriber Information*, we ask Parliament to send a clear message to *all* telecommunications providers outlining how they are to conduct themselves by enacting legislation that makes it clear that warrants are required for telecommunications companies to disclose personal information, including subscriber information. Those requests and disclosures of such information should be recorded and reported in order to preserve accountability.

The need for such a clear message is obvious when one considers the sheer number of warrantless requests that were being made prior to *Spencer*, as well as the number of requests with warrants that have been made since. While it is not the case that state officials *never* obtained warrants prior to *Spencer*, it was routine to make requests for voluntary disclosure. In 2013 alone, government agencies made 87,856 requests for voluntary disclosure of subscriber information and 711 requests for assistance in child exploitation investigations to Rogers.[36] Telus received some 40,900 requests for subscriber information in the same year.[37] Following *Spencer*, some Canadian service providers have complied with the verdict and voluntarily released transparency reports – revealing the number of subscriber information requests made annually, as well as the number of requests complied with or refused.[38] In keeping with *Spencer*, Rogers and Telus show that the number of voluntary disclosures had dropped to 0 per year after the decision. Telus, TekSavvy and Shaw all indicate they are making efforts to investigate the reasonableness of information requests, even when a warrant is given, and denying those that are overly broad or compromise the privacy interests of too many customers.[39] (We note with some concern that Bell, one of the largest service providers, has yet to release a transparency report or adopt a position with respect to the ruling in *Spencer*.)

---

[34] *Ibid* at para 15.
[35] S 487.0195 *Criminal Code.*
[36] Rogers Communications, *2013 Transparency Report* <https://www.rogers.com/cms/images/en/S35635%20Rogers-2013-Transparency-Report-EN.pdf>.
[37] Telus, *Telus Transparency Report 2013* <http://about.telus.com/servlet/JiveServlet/previewBody/5544-102-1-6081/TELUS%20Transparency%20Repo%20r>.
[38] Though there is no prescribed form for such transparency reports, the *Transparency Reporting Guidelines* released by Industry Canada set out a general template for service providers in order to make their data easily comparable. For the template, see Industry Canada, *Transparency Reporting Guidelines*, June 30, 2015. <http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html>.
[39] TekSavvy, *TekSavvy Transparency Report – In Response to Citizen Lab*, June 4, 2014. <https://teksavvy.com/en/why-teksavvy/policies/legal-stuff/transparency-report>. Rogers Communications, *2015 Rogers Transparency Report*. http://about.rogers.com/about/helping-our-customers/transparency-report. Telus, *Telus Sustainability Report 2015*, p. 131, <https://sustainability.telus.com/en/business-operations/transparency-report/>. Shaw Communications Inc.,

The Fallibility of Warrants

In addition to the problematic conflation of subscriber information within the metadata regime, and the need for consistent standards for access by law enforcement, it is important to recognize that warrants themselves are fallible and can provide little protection. The recent Federal Court decision revealing CSIS' decade-long, widespread, breach of our privacy rights by illegally sharing and retaining metadata starkly illustrates that even the existence of a warrant regime can fail to protect us.[40]

Even when law enforcement follows the proper procedure to seek a warrant, warrants themselves may offer only illusory protection of our privacy. This was evidenced by a Canadian study, which found that at least 61% of warrants would not have passed constitutional muster if challenged under a section 8 application – in other words, they never should have been issued in the first place.[41]

We echo the concerns raised by stakeholders and experts that government agencies must have firm rules to address how digital information can by lawfully used, retained, shared and destroyed after it is initially acquired. **In revising our current system, or in creating a new one, warrants must extend to protect and outline what can be done with our information after it is lawfully acquired**.[42] Accountability over the use and retention of information is critical, and is especially deficient in the national security context.

The Need for Greater Post-Collection Accountability

With Bill C-51, government intelligence retention and sharing has been expanded through the *Security of Canada Information Sharing Act* (SCISA). Under this legislation, all government agencies are granted authority to share any information with the listed 17 recipient organizations *on their own initiative* if they deem that information to be *relevant* to activities that "undermine the security of Canada".[43] While the free and expedient flow of information may be vital to protect national security interests, the ill-defined standard for information sharing must be cautiously balanced with our fundamental rights and freedoms. We have advocated for a system of prior authorization, but after information is obtained, we also need to achieve this balance through a robust, independent system of review. The existing accountability measures over the sharing and retention of digital information are inadequate, especially so in the national security context.

Transparency, online at p. 1. https://www.shaw.ca/uploadedFiles/Privacy_Policy/Shaw_Transparency_Report_2015-_FINAL.pdf.

[40] *In the Matter of An Application By… For Warrants Pursuant to Sections 12 and 21 of the Canadian Security Intelligence Act…*, 2016 FC 1105.

[41] Casey Hill, Scott Hutchison, & Leslie Pringle, "Search Warrants: Protection or Illusion?" (2000) 28 C.R. (5th) 89 (WL).

[42] *False Security, supra* note 32 at 123.

[43] *Security of Canada Information Sharing Act*, SC 2015, c 20, s 5(1).

The Privacy Commissioner Needs Resources and Power

The *Privacy Act* provides guidelines on how government institutions can handle personal information. The purpose of the act is to "protect the privacy of individuals with respect to personal information about themselves held by a government institution and [to] provide individuals with a right of access to that information".[44] Section 8(1) of the bill prohibits the disclosure of personal information without consent.[45] However, section 8(2)(a) qualifies an exception that disclosure may be permitted "for the purpose for which the information was obtained … or for a use consistent with that purpose".[46] In this way, Bill C-51 effectively neutralizes these protections by authorizing the disclosure for a broad range of national security interests.

The Privacy Commissioner is an independent agent of Parliament tasked with overseeing the compliance of *all public bodies* with the provisions of the Act. Bill C-51's abatement of the *Privacy Act* is exacerbated by a lack of resources and limited mandate of the Privacy Commissioner, who can provide little oversight for intelligence sharing within and among government.[47] The Office of the Privacy Commissioner (OPC) released a report stressing its inability to effectively oversee the sharing of information between agencies. One problem is that its mandate is outdated; "unrevised since 1983".[48] Of course, the existence of modern national security threats and the development of technology that advances seamless intelligence sharing was not anticipated when the Privacy Commissioner's role was created. Given Bill C-51's enhancement and integration of law enforcement powers when it comes to sharing information, there is a corresponding need for enhanced and integrated oversight.[49] It simply is not feasible for one body to oversee the distribution of intelligence between seventeen agencies of a much larger magnitude.

The Silo-ing of Independent Review Bodies

In addition to the Privacy Commissioner, there are three independent review bodies that seek to hold their respective agencies accountable for information sharing: the Security Intelligence Review Committee (SIRC) for the Canadian Security Intelligence Service (CSIS), the Civilian Review and Complaints Commission (CRCC) for the Royal Canadian Mounted Police (RCMP), and the Office of the Communications Security Establishment Commissioner (OSEC) for the Communications Security Establishment (CSE).[50] These three review bodies have a mandate to exclusively review and investigate their corresponding agency. This helps to address the challenges faced by the OPC with regards to monitoring an expansive network of intelligence sharing by establishing a one-to-one relationship between agency and review body. However, because the

[44] *Privacy Act*, RSC 1985, c P-21, s 2.
[45] *Ibid* at s 8.
[46] *Ibid* at s 8(2)(a).
[47] Craig Forcese & Kent Roach, "Bridging the National Security Accountability Gap: A Three-Part System to Modernize Canada's Inadequate Review of National Security" (2016) The Canadian Network for Research on Terrorism, Security, and Society Working Paper Series No 16-04 at 13 ["Bridging the Gap"].
[48] Office of the Privacy Commissioner of Canada, *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (Ottawa: Minister of Public Works and Government Services Canada, 2014) at 5.
[49] *Ibid.*
[50] *Green Paper supra* note 2 at p 10.

review bodies do not have jurisdiction beyond their particular agency, they are unable to conduct joint investigations, which is particularly troublesome considering the agencies they are responsible for have a heavily collaborative information sharing process. This 'silo' effect impedes the ability of these review bodies to conduct thorough reviews.[51] Further, these independent bodies only cover three of the agencies engaged in information sharing; the other agencies that have been conferred powers in Bill C-51 do not yet have particular review bodies to hold them accountable.

There is also evidence that these review bodies neither have adequate access to, nor understanding of, the internal operations of their respective agencies. For example, in SIRC's 2015 annual report, it was found that CSIS "had no record of the deliberations surrounding the managerial assessments" and that "given the absence of documentation, SIRC found it difficult to make a complete assessment of the decisions taken at the management level".[52] Further, even assuming these review bodies are able to recognize the extent to which their respective agencies are behaving lawfully, they are not mandated to consider the efficacy of these agencies – whether their operations are actually helping extinguish threats to national security. Thus, they are unable to determine whether the provisions of Bill C-51 actually have a beneficial effect on threat reductions.[53]

Ministerial Accountability and Its Limitations

The Minister of Public Safety and Emergency Preparedness and the Minister of National Defence are tasked with the oversight of some national security agencies.[54] Through issuing Ministerial Directions (MDs), they are able to "establish guidelines" regarding the use of intelligence.[55] However, this oversight is susceptible to the same inadequacies as the OPC; that is, among other things, they lack both the resources and understanding to sufficiently conduct a review of a massive network of information use and distribution. Additionally, there is the clear concern of tasking the executive with criticizing its own actions.[56] In order to avoid coming under their own scrutiny, Ministers may hesitate to reveal both the propriety and efficacy shortcomings of the very agencies for which they are responsible.

Parliamentary Review: The Proposed Solution for the Accountability Gap

Expanding the role of the Parliament could help bridge the national security accountability gap. However, "Canada is alone among its "Five Eyes" partners…in not giving any parliamentarians (other than ministers) routine access to secret information".[57] This is troublesome when those tasked with drafting legislation are unable to openly access the operations to which the legislation is concerned. Without full access

[51] "Bridging the Gap", *supra* note 47 at 13.
[52] Security Intelligence Review Committee, *SIRC Annual Report 2015-2016: Maintaining Momentum* (Ottawa: Public Works and Government Services Canada 2015) (Chair: Pierre Blais).
[53] "Bridging the Gap", *supra* note 47 at 20.
[54] According to Green Paper, *supra* note 2, the Minister of Public Safety is responsible the Canadian Border Services Agency, CSIS, and the RCMP, while the Minister of National Defence is responsible for the Communications Security Establishment, the Department of National Defence, and the Canadian Armed Forces.
[55] *Green Paper, supra* note 2 at 9.
[56] "Bridging the Gap," *supra* note 47 at 20.
[57] *Ibid.*

to information, Parliament's ability to hold intelligence agencies accountable is effectively undermined. The government has expressed awareness of this issue and has tabled Bill C-22, the *National Security and Intelligence Committee of Parliamentarians Act*, "to create a national security and intelligence committee of parliamentarians with broad access to information".[58] According to Forcese and Roach, this could allow for "a whole of government mandate to match the government executive's whole of government approach to security".[59] Of course, the efficacy of such a Parliamentary committee hinges on several contingencies which have already been shown to plague the existing review bodies: inadequate resourcing and expertise, inability to cooperate with other review bodies and intelligence agencies, and a lack of transparency. Given the success of similar oversight committees in other countries, as will be described in Part IV below, it appears that these concerns are manageable.

The Heightened Importance of Accountability in the National Security Context

Clearly, post-collection accountability is particularly deficient in the national security context. Troublingly, it is this context where accountability is most important. In the national security context, greater post-collection accountability might be able to ameliorate (a) heightened risks of more severe rights violations, (b) the more serious security threats at stake, and (c) the limited opportunities for government transparency.

(a) Heightened Risk: Rights Violations

To demonstrate the heightened risks of more severe rights violations, consider the following example:

> CSIS gains access to subscriber information about A. They find that A has been in regular communication with B, who is associated with a terrorist organization. CSIS does no further investigation into A, and does not do anything to verify A's relationship with B. At a later date, CSIS casually relays A's connection to terrorist organizations to a foreign party, who arrests A and tortures her into providing evidence against B. In fact, the communication between A and B was never related to any terrorist offences. A and B were merely friends, and A had no idea whatsoever about B's alleged involvement with terrorist organizations.

Information collected for national security purposes is often shared with foreign parties, and these foreign parties might not always share our values. We must bear in mind the risks of sharing information collected about Canadians. Unfortunately, Canada experienced an incident like this in 2002, when Canadian citizen Maher Arar was deported to Syria and tortured. The inquiry into Arar's deportation revealed the RCMP had provided American authorities with inaccurate information about Mr. Arar, "in ways that did not comply with RCMP policies requiring screening for relevance, reliability and personal information".[60] Greater oversight and accountability could prevent rights violations in cases like these. In the Arar case, it might have ensured that the RCMP complied with its own standards, and guarded against the sharing of misleading information.

[58] *Green Paper, supra* note 2 at 11.
[59] "Bridging the Gap", *supra* note 47 at 19.
[60] 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,* by Justice Dennis O'Connor (Ottawa: Publishing and Depository Services, 2006) at 13.

(b) Heightened Risk: Security

To demonstrate the heightened risks of security, consider the following example:

> Suppose CSIS collects the same subscriber information about A, but after further investigation realizes there is no reason to believe A is actually involved with terrorist activity. CSIS takes A off their radar. Meanwhile, the police are conducting a separate investigation and they decide to question A because of her communication with B. They spend long hours interrogating and investigating A, trying to gain valuable information. CSIS knows that the police are likely following a dead end, but they do not share their information about A. As a result, the police waste their time on the wrong suspect, and fail to identify the real threat. As a result, a terrorist attack is committed on Canadian soil in the meantime.

While law enforcement is bound to sometimes follow dead ends, we should aim to minimize these occurrences whenever possible. This is especially true in cases involving threats to national security, where the nature of the threat is such that they usually pose a larger risk of harm to a larger number of Canadians. Nonetheless, decisions about whether to share information across agencies can be complex. CSIS has expressed concern about classified intelligence being leaked through the process of disclosure if it is shared with law enforcement.[61] Greater accountability over the use and retention of personal information can help ensure that the costs and benefits of sharing information between agencies are carefully weighed. Presently, there is no system of whole-of-government review that could effectively hold security and intelligence agencies accountable for the way in which information is shared.[62]

(c) Heightened Risk: Loss of Public Confidence

In the national security context, where information is often sensitive and classified, government transparency is inherently less possible. As a result, the government cannot be fully candid about what information it retains after collection and how that information is used. Canadians must accept a certain amount of secrecy in these matters as being for their own benefit. However, this makes it all the more important to ensure that Canadians can have faith in the system. Canadians must be able to have confidence that there is an adequate system of review and oversight in place that will effectively prevent the government from abusing its power and control of their personal information. A strong system of oversight and review that can keep the government accountable for the way it uses personal information, might better ensure public confidence.

In sum, Part III of this submission has made clear that the the current system of privacy protections is notably lacking. Canada needs to reaffirm the need for judicial authorization for government access to subscriber information subject to exigent circumstances. However, the exception of "exigent circumstances" acknowledged in *Spencer*, needs to be clearly and narrowly defined. Sharing between government institutions needs to be limited by a clear and reasonable threshold that must be met before information can be shared. This threshold should meet the standard required by the recipient agency's governing statute. Information

[61] *False Security, supra* note 32 at 290.
[62] "Bridging the Gap", *supra* note 47 at 4.

sharing should be recorded and subject to review by the proposed review system. Finally, Canada requires a review system sufficient to ensure that access to Canadians' information is not subject to abuse and then covered by the secrecy of national security. In other words, Parliament needs to respect the constitutional parameters of section 8 *Hunter*, implement a clear and reasonable threshold consistently across agencies and regimes, and enhance post-collection accountability.

Part IV: Lessons from Abroad

In this Part of our submission, we review some of the approaches that have been undertaken by other jurisdictions in their attempts to protect privacy rights when national security interests are involved. We undertook this review in order to make recommendations as to how Canada could best create a constitutionally sound system for attaining basic subscriber information in the national security context.

By looking to Australia, the U.S., the U.K., and Germany, Canada can benefit from the experiences these countries have in trying to implement national security programs that respect privacy. It should be noted that none of these countries' approaches should be adopted in their entirety. They each possess strengths and weaknesses. Rather, Canada should learn from the positive steps these countries have taken to protect privacy rights in the national security context. Similarly, Canada can also learn from the missteps they took along the way. Canada should not look to emulate programs that have been criticized for blatantly infringing the privacy rights of their citizens. Protection of privacy is not a game of follow the leader, wherever they may go. Canada should learn from the critiques of other countries and do better, always mindful of the importance of the Canadian Charter as the basic protection of our rights.

Lesson 1: The Need for Protection in Retention

Around the world, data retention legislation has become a focus area for national security and criminal justice initiatives. Data retention schemes tend to outline a period of time that service providers are required to maintain data, often under the framework that data may assist in criminal investigations and prosecutions.[63] These types of retention laws have substantial negative impacts on privacy rights. Countries that have enacted these data retention programs have been met with significant critique. Longer retention increases the risk of breach and thus individuals' privacy interests are jeopardized.[64] Mass requirements effect law-abiding citizens who have done nothing to justify the infringement.

In Germany, for example, public service providers are required to retain customer data for a minimum period of 10 weeks for call detail records and internet metadata.[65] The law in Germany also requires that the data be erased once the retention period expires, due to which they have been praised as being "privacy

[63]Clarke, Roger, "Data Retention as Mass Surveillance: The Need for an Evaluative Framework," (2015) 5:2 International Data Privacy Law 121 at 121
[64] Sarah Tracey, "The Fall of the Data Retention Directive," (2015) 20:2 Communications Law 53 at 54.
[65] Eric Shinabarger, "New German Data Retention Law Expected to Take Effect Soon," (13 January 2016) *Lexology – Privacy Law Corner* (blog), online: < http://www.lexology.com/library/detail.aspx?g=fe41234a-b807-47da-a20e-b725327b537a> .

conscious".[66] In Australia, information necessary to identify the owner of a telecommunications account must be kept from creation until at least two years after the termination of the account or service.[67] In enacting its legislation, Australia sought to address the concern of increased risk attached to their lengthy retention period with the inclusion of encryption requirements with a fund to help companies develop stronger protection mechanisms.[68] Other countries, such as the U.S., have attempted to enact mandatory retention schemes but have not been successful in doing so.[69]

Under the U.K.'s previous and new legislation, the Secretary of State can serve notice to telecommunication companies that compels them to retain data for up to 12 months.[70] This model is similar to the framework Canada has enacted in the *Protecting Canadians from Online Crime Act*.

If Parliament chooses to enact a data retention scheme, as it discusses in the *Green Paper*,[71] it must proportionally balance the interests that law enforcement and security agencies have in preservation of data with the individual and societal interest in privacy protection. Legislation must reflect the clear statement from *Spencer*: that Canadians have a privacy interest in remaining anonymous online. Minimum retention periods, as seen in Germany; requirements and funding for encryption, as seen in Australia; and target-specific retention as seen in the U.K. and current Canadian legislation – these are all possible avenues for Canada to rely on if it enacts a data retention scheme. It is important that whichever avenue Canada chooses, it must ensure that access to retained data is rigorously restricted though the following measures:

- **Canada should not enact widespread a mandatory minimum retention period, as is alluded to by the *Green Paper*, given the significant risk it poses to the privacy of law abiding citizens.**
- **If Canada enacts a mandatory minimum retention period, it should be as short as possible. We recommend following the lead of Germany and setting the minimum at 10 weeks.**
- **If a mandatory minimum retention period is enacted, Canada should also mandate strong encryption requirements and provide funding to service providers to implement those requirements.**
- **Canada should match any retention requirements with mandated maximum periods of retention, as adopted in German legislation.**
- **As will be discussed below, Canada should match retention with requirement of judicial authorization to access to this information, and independent review of use information once obtained.**

---

[66] Jones Day, "The Data Retention Saga Continues: European Court of Justice and EU Member States Scrutinize National Data Retention Laws," (11 August 2016) *Lexology*, online: <http://www.lexology.com/library/detail.aspx?g=a886514b-71ab-4779-a2e7-d1486076e01b>
[67] *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth). s187C [*Telecommunications Amendment*].
[68] *Ibid* at s187BA.
[69] See US, Bill HR 1076, *Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009*, 111th Cong, (2009).
[70] *Data Retention and Investigatory Powers Act 2014* (UK), c27, s1; Bill no 143, *Investigatory Powers Bill* 2015-2016 sess, 2016 s78 [*Investigatory Powers Bill*].
[71] Green Paper, *supra* note 2 at 57

Lesson 2: The Need for Judicial Authorization

As discussed above, *Spencer* held that Canadians have a privacy interest in their anonymous use of technology. In some circumstances, this requires police to produce warrants to access subscriber information held by service providers. We recommend that Canada's warrant and production order standards be maintained to protect these important privacy interests.

Spencer goes further to protect privacy values where other countries fall short by restricting access to subscriber information. In Australia, warrantless access is allowed, but recent changes have restricted access to criminal law enforcement agencies.[72] In January 2016, the Australian government released a list of 60 governmental agencies from all levels that had applied for reclassification as a "criminal law investigation agency" to try and regain that access.[73] The government has denied each of these requests.[74] In the U.K., subscriber information and other metadata was accessible by a large number of government departments through a request from a senior official to the communication service provider.[75] The U.K. is in the process of passing the *Investigatory Powers Bill*, which has moved to include judicial oversight of warrant applications but continues to grant warrantless access to communication data by senior officials of public authority when in relation to national security.[76]

Looking abroad, warrantless access to metadata in some capacity has been largely accepted by governments. The *Spencer* ruling presents Canada with the opportunity to operate at a higher standard by recognizing the importance of anonymity and the privacy interest in that data. Parliament should take this opportunity to maintain the higher standard of privacy protection.

As noted above the *Spencer* decision recognizes that there is an "exigent circumstances" exception in which police can conduct warrantless searches where warrants would otherwise be required.[77] In the context of a national security threat, where harm to the public is imminent, this exception would apply. Concerns about time constraints are significantly minimized by the exception. As stated by the OPC,

---

[72] Australian, Commonwealth, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Parl Paper No 170 (2013) at 161. [*Report of the Inquiry*]
[73] Stephanie Anderson, "List of agencies applying for metadata access without warrant released by the Government," *Australian Broadcasting Corporation* (17 January 2016), online: <http://www.abc.net.au/news/2016-01-18/government-releases-list-of-agencies-applying-to-access-metadata/7095836>.
[74] Benjamin Sveen, "Data Retention Bill: Government Departments ask AFP to access metadata after legislation enacted," *Australian Broadcasting Corporation* (3 October 2016), online: <http://www.abc.net.au/news/2016-10-04/government-departments-obtain-metadata-via-afp/7898648>. [Data Retention Bill]
[75] Brown, Dan, "Regulation of Converged Communications Surveillance," in D. Neyland and B Goolds, eds, *New Directions in Surveillance and Privacy* (Exeter, UK: Willan, 2009) 39 at 45-46. This is modified by the incoming *Investigatory Powers Bill, supra* note 70.
[76] *Investigatory Powers Bill*, *supra* note 70, s53
[77] *Spencer*, *supra* note 18 at paras 71-74.

> *"…it is unclear to us why neither the evidentiary threshold required to obtain judicial authorization via production order or warrant nor the exigent circumstances exception articulated in R. v. Spencer, can be met."*[78]

For this reason, Parliament should maintain the requirement of judicial authorization for access to subscriber data. Subject to exigent circumstances, all legislation should, on its face and in effect, adhere to the requirement of judicial authorization to access individual's information. To protect against potential overreach of the exception, we recommend that Parliament clarifies what constitutes "exigent circumstances" and requires judicial review over searches that fall into this category. Parliament should also mandate that service providers are not to release this information in the absence of judicial authorization. By taking these steps, Canada can be a global leader in its protection of privacy rights in the technological sphere.

Lesson 3: The Need for Strong Sharing Boundaries

It is not sufficient for Parliament to protect Canadians privacy only at the access stage of an investigation. Our government must ensure that Canadians' information, once accessed, is not distributed in a way that violates our privacy interests. As our preceding section explained, SCISA grants any government agency the power to share information with one of the 17 listed recipient institutions if information is "relevant" to the national security responsibilities of the recipient.[79]

Germany facilitates information sharing through a departmental discretion approach. There is a common data base that 38 government agencies contribute and have access to. Information in the database is sorted into "open" and "concealed" storage.[80] Information in open storage can be searched by a participant agency.[81] A search for a name in open storage will reveal any relevant information.[82] A search for a name that is in closed storage will not reveal any information.[83] In the latter case the agency that has stored the information will be notified of the search, and will determine if they are able to share the information with the searcher.[84] This approach is problematic as there is no oversight or review of sharing. Its complete discretion puts it at risk of being both overbroad and too narrow. To address these issues, highlighted in Germany, Canada must set clear sharing standards and implement a review mechanism.

---

[78] Daniel Therrien, "Appearance before the Standing Committee on Public Safety and National Security (SECU) on Public Safety's Green Paper," *Office of the Privacy Commissioner of Canada* (Advice to Parliament) (4 October 2016), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2016/parl_20161004/>.
[79] *Anti-Terrorism Act, 2015*, S.C. 2015, c. 20, s2, ss5(1), "Sch.3", 9.
[80] *Gesetz zur Errichtung einer standardisierten zentralen Antiterrordatei von Polizeibehörden und Nachrichtendiensten von Bund und Ländern* , *Geändert durch Art. 5 G v. 26.2.2008 I 215*
[81] Paul M. Schwartz, "Systematic Government Access to Private-Sector Data in Germany," (2012) 2:4 International Data Privacy Law 289 at 296.
[82] *Ibid.*
[83] *Ibid.*
[84] *Ibid.*

In Australia, an investigative report found that some departments that had lost their warrantless access to metadata, submitted requests to the Australian Federal Police (AFP) to conduct the searches on their behalf and pass on the information.[85]

The example from Australia highlights a problem with open information sharing: it allows agencies and departments to access information when they have not met their threshold required to do so by having other agencies with lower threshold requirements obtain the information. Under SCISA, Canada's government agencies are potentially susceptible to similar problems. Federal departments who have lower thresholds to lawfully access information may be able to share it with those that have higher thresholds, getting around the recipient agencies' standards. It may be that SCISA is interpreted to negate this potential problem, but at this time it is unclear whether this kind of information sharing would be allowed.

For these reasons we recommend that Parliament limit information sharing between agencies by implementing clear and reasonable standards on information sharing that are consistent with and adhere to the recipient's standard for access.[86] For example, information shared with CSIS should be 'strictly necessary' to their national security objective, as this is the threshold for their collection and retention of information.[87] To ensure compliance with these standards, we recommend that information sharing is included in the mandate of review bodies, which will be discussed below.

Further, given that *Wakeling v. United States of America* established that information sharing and disclosure can be subject to *Charter* protection under section 8[88], agencies should be required to maintain records of requests, sharing and disclosure. Where compatible with national security, notice of the disclosure to the person whose information is requested, disclosed and shared should also be provided. These records should be subject to review, under the 3-part system outlined below.

Lesson 4: The Need for Stronger Review

As we have shown, Canada's current review system does not adequately protect Canadian privacy interests, nor does it ensure that national security agencies are properly using their investigatory powers.

Though flawed in other aspects of their national security approach, Australia and the U.K. have recently enacted strong review systems. As such, they provide positive models for reform of the Canadian review approach.

[85] Sveen, "Data Retention Bill" *supra* note 74.
[86] Daniel Lang, "Bill C-51, the *Anti-Terrorism Act, 2015*: Submission to the Standing Senate Committee on National Security and Defence," *Office of the Privacy Commissioner of Canada* (16 April 2016), online: < https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150416/>.
[87] *Ibid.*, retention requirement found in 2016 FC 1105
[88] *Wakeling supra* note 7 at para 40

Australia has a three-part review body. It has an independent inspector that reviews the activities of all Australian security and intelligence agencies.[89] Australia also has an Independent National Security Law Monitor comprised of non-government lawyers who can hold hearings, see classified information, and issue reports on the government's anti-terror laws.[90] Finally, Australia has a Parliamentary Joint Committee on Intelligence and Security, which has access to confidential documents in its oversight role.[91]

The U.K. similarly has a strong review framework. The *Investigatory Powers Bill*, which is set to become law by the end of the year, combines three separate oversight roles into a single Investigatory Powers Commissioner.[92] The U.K. has an independent reviewer of terrorism legislation who is given "unrestricted access" to security information and personnel.[93] The Intelligence and Security Committee is a parliamentary committee responsible for the oversight of the U.K.'s intelligence agencies.[94]

Following the examples of Australia and the U.K., we recommend that Canada strengthens our review system through a three-part system.[95] **First, Parliament should pass the currently tabled Bill C-22 which will create a Parliamentary review committee.** This would reintegrate national security initiatives into our democratic system.

Second, Canada should instate an independent legislative reviewer to provide Parliament and the public the information required to assess future legislative initiatives. Bill C-22's mandate includes the ability to review legislative and regulatory initiatives. However, Canada would benefit from an expert body committed to evaluating the legislative framework as well.

Finally, Parliament should instate an independent review body with a mandate as broad as the collaboration between the security agencies it oversees. This would realign with recommendations from previous review commissions that Canada requires a comprehensive approach that is not tied to a single agency.[96] **This review body should also be responsible for evaluating the possible section 8 infringements that have to potential to arise from disclosure of constitutionally acquired information.** Only when a comprehensive review framework is enacted will national security agencies be held accountable, and Canadians' privacy be adequately protected.

[89] "Bridging the Gap" *supra* note 47 at 33.
[90] *Ibid* at 3, 37, 56.
[91] *Ibid* at 16, 32.
[92] *Investigatory Powers Bill*, *supra* note 70, s194.
[93] See Independent Reviewer of Terrorism Legislation, "The Independent Reviewer's Role" (2013) online: <https://terrorismlegislationreviewer.independent.gov.uk/about-me/>.
[94] See U.K., "Intelligence and Security Committee of Parliament," (2016) online: <http://isc.independent.gov.uk/>
[95] This recommendation is derived from the approach forwarded by Craig Forcese and Kent Roach's "Bridging the Gap" *supra* note 47.
[96] *False Security, supra* note 32 at p 442 – discussion of the recommendations from the Arar Commission.

Conclusions

Our expectation is for government to protect us from national security threats. That protection cannot come at the expense of our fundamental rights and freedoms guaranteed by the *Charter*. In this vein, we agree that law enforcement must be able to act promptly to protect us when our national security is at stake – but we insist that such quick action be justified, before it occurs, to an impartial and independent decision maker on objectively reasonable grounds. Regardless of what ultimate form that prior authorization takes, these seminal constitutional principles must be observed. Unfortunately, the *Green Paper*'s proposals to streamline access to search warrants in cases where national security is at stake would result in our Charter rights being unjustifiably infringed.

We submit that modernizing the traditional warrant system in a manner that aligns with the constitutional parameters of section 8 can meet the efficiency needs of national security context, while also protecting the guaranteed privacy rights enshrined in the *Charter.* We underscore the pertinence of systemic reform to warrantless access for subscriber information, as the search and seizure protections of section 8 do not end when police obtain a warrant.[97] As the Supreme Court stressed in *Wakeling*, information sharing with foreign states for law enforcement purposes may trigger a residual expectation of privacy and attract *Charter* scrutiny.[98] Consequently, a proactive approach to address deficiencies now can enhance the protections for the future, but also for guarding against *Charter* violations and subsequent costly litigation. We encourage Parliament to avail of this opportunity to improve the overall existing scheme for national security and to address the consistency and accountability problems that plague the legislative regime.

[97] *Mills, supra* note 8 at para 108
[98] *Wakeling, supra* note 7.