Court File No.: CV-14-504139

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION AND CHRISTOPHER PARSONS

Applicants

- and -

HER MAJESTY THE QUEEN IN RIGHT OF CANADA AS REPRESENTED BY THE ATTORNEY GENERAL OF CANADA

Respondent

FACTUM OF THE APPLICANTS, CANADIAN CIVIL LIBERTIES ASSOCIATION AND CHRISTOPHER PARSONS

Paliare Roland Rosenberg Rothstein LLP
155 Wellington Street West
35th Floor
Toronto, ON M5V 3H1

Andrew Lokan (LSO #31629Q)
Tel.: 416.646.4324
email: andrew.lokan@paliareroland.com

Kartiga Thavaraj (LSO #75291D)
Tel.: 416.646.6317
email: kartiga.thavaraj@paliareroland.com

Fax: 416.646.4301

Lawyers for the Applicants

TO: **Attorney General of Canada**
Department of Justice
The Exchange Tower
130 King Street West
Suite 3400, Box 36
Toronto, ON M5X 1K6
Tel: 416.573.4637

Laura Tausky
email: Laura.Tausky@justice.gc.ca

Marilyn Venney
email: marilyn.venney@justice.gc.ca

Fatemah Khalfan
email: fatemah.halfan@justice.gc.ca

AND TO: **Attorney General of Ontario**
Constitutional Law Branch
McMurtry-Scott Building
720 Bay Street, 4th Floor
Toronto, ON M7A 2S9
Tel: 416.455.5189

Waleed Malik
email: waleed.malik@ontario.ca

Sean Hanley
email: sean.hanley@ontario.ca

Intervenor

AND TO: **The Privacy Commissioner Of Canada**
30 Victoria Street, 8th Floor
Gatineau, QC K1A 1H3
Tel: 819.775.8044

Rebecca De Sanctis
email: rebecca.desanctis@priv.gc.ca

Sarah Speevak
email: sarah.speevak@priv.gc.ca

Intervenor

TABLE OF CONTENTS

PART I. OVERVIEW 2
PART II. FACTS 4
A. The Parties 4
B. The Applicants' Witnesses 5
C. Procedural Background 5
D. Legislative Framework 6
E. The Impugned Provisions 8
F. Basic Subscriber Information 10
G. TSPs' Disclosure of Information 11
H. Lawful Authority 13
I. An Individual's Knowledge of an Information Request 17
J. Information Collected Pre-Spencer 19
PART III. ISSUES 19
PART IV. LAW AND ANALYSIS 20
A. The Applicants' Standing 20
B. The Impugned Provisions Violate Section 8 20
1. Overview of Section 8 20
2. Basic Subscriber Information and a Reasonable Expectation of Privacy 21
3. The disclosure regime in *PIPEDA* is not reasonable 23
C. The Impugned Provisions Violate Section 7 26
1. The Provisions Violate the Right to Liberty and Security of the Person 26
2. The Violation of the Right to Liberty and Security of the Person Is Not in Accordance with the Principles of Fundamental Justice 28
D. The Veto Powers Violate s. 2(b) 30
E. The Impugned Provisions are not saved by s. 1 31
F. The Appropriate Remedy 33
PART V: Conclusion 34

PART I. OVERVIEW

1. The Applicants challenge the constitutional validity of certain sections of the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"),[1] which facilitate and permit the warrantless disclosure of basic subscriber information by private telecommunications service providers ("TSPs") to government institutions.

2. Sections 7(3)(c.1), 9(2.1), 9(2.2), 9(2.3) and 9(2.4) of *PIPEDA* (the "Impugned Provisions") enable government agencies to acquire personal information that is subject to a reasonable expectation of privacy without the consent of the individual whose information is sought, and then allow the government to require the private organization to withhold the fact that the individual's information was requested. While s. 7(3)(c.1) requires that the agency identify its "lawful authority" to the TSP when requesting information, and the Supreme Court of Canada ("SCC") ruled in *R. v. Spencer*[2] ("*Spencer*") that *PIPEDA* itself does not supply that authority, in practical terms there are no real or adequate protections against disclosure. These requests are not subject to judicial scrutiny and there is little reason to believe that the individuals affected would even be aware of the requests.

3. Most individuals whose information has been disclosed will only be made aware of the disclosure if either (1) they proactively seek out the information *and* a government institution does not block their request for information, or (2) if they face criminal charges. The Privacy Commissioner ("Commissioner") and Office of the Privacy Commissioner

[1] *Personal Information Protection and Electronic Documents Act,* S.C. 2000, c. 5.
[2] 2014 SCC 43 ["*Spencer*"].

("OPC") have an oversight role, but it is severely limited by an absence of transparency and meaningful accountability mechanisms.

4. Prior to *Spencer*, government agencies requested and received information from TSPs on a massive scale, as these agencies and the TSPs incorrectly assumed that *PIPEDA* itself authorized the collection. Post-*Spencer*, the volume of requests to TSPs and their disclosure to the agencies appears to have gone down, but it still occurs in the absence of adequate controls. Moreover, the agencies took no steps to delete or destroy their stockpiles of personal information that was collected before the SCC clarified the interpretation of "lawful authority". The Applicants have identified six federal agencies that account for the bulk of the requests within federal jurisdiction—the Canadian Border Services Agency ("CBSA"), the Royal Canadian Mounted Police ("RCMP"), the Canadian Security Intelligence Service ("CSIS"), the Communications Security Establishment ("CSE"), the Canada Revenue Agency ("CRA") and the Competition Bureau.

5. The protection provided by the *Charter* for privacy is essential not only to human dignity, but also to the functioning of our democratic society. The Applicants assert that the Impugned Provisions violate sections 8, 7 and 2(b) of the *Charter*. Collectively, they authorize and facilitate unreasonable searches and seizures, contrary to s. 8. They are vague, overbroad and arbitrary and the gathering and storage of personal information under these provisions violate individual liberty and security of the person, contrary to s. 7. To the extent that they prevent individuals from learning about disclosure of personal information to a government agency, they also infringe s.2(b). These infringements are not demonstrably justified in a free and democratic society.

6. The Applicants seek declarations of invalidity, and an order that the pre- and post-*Spencer* stockpiles of information collected contrary to the *Charter* be deleted and destroyed. Alternatively, the Applicants request guidance on the meaning of "lawful authority" and on the manner in which the legislation should work to ensure that the rights of individuals are preserved as far as possible when government agencies request information from TSPs for which individuals have a reasonable expectation of privacy.

PART II. FACTS

A. The Parties

7. The Canadian Civil Liberties Association ("CCLA") has long been involved in protecting civil liberties in Canada, including with respect to privacy, liberty, security of the person and freedom of expression. The CCLA brings this application as a public interest litigant. Dr. Christopher Parsons ("Parsons") is an academic who has studied federal government policy and legislation respecting personal information and privacy with a focus on electronic data. When the application was commenced, he was a post-doctoral fellow at Citizen Lab, at the Munk School of Global Affairs & Public Policy, University of Toronto.[3] The Respondent Attorney General of Canada ("AGC") is responsible for defending federal legislation in the courts. The Attorney General of Ontario ("AGO") has intervened as of right, and the OPC was granted leave to intervene in November of 2017.[4]

[3] Affidavit of Christopher Parsons, sworn April 29, 2015 ["Parsons 1st Affidavit"], Application Record ["CCLA Record"], Vol. 1, Tab 4, at para. 1.

[4] *Canadian Civil Liberties Association v. Canada*, Order of Belobaba J., dated November 10, 2017 at para. (a), Supplementary Application Record ["SAR"], Tab 7.

B. The Applicants' Witnesses

8. Dr. Parsons has provided three affidavits. His research interests include the relationship between telecommunications service providers ("TSPs"), internet service providers ("ISPs") and government agencies (including law enforcement agencies and national security agencies). He has expertise on issues of privacy as they relate to the relationship between TSPs (including ISPs) and government agencies. He has conducted studies to gather information about TSPs' data retention and sharing policies and has made his own personal requests for such data.[5] Dr. Michael Geist, who provided one affidavit, is a law professor with a focus on law and technology. He has expertise on the practical workings and policy implications of privacy legislation in the context of TSPs and their relationship with government agencies.[6] Sukanya Pillay, former Executive Director of the CCLA, has provided an affidavit addressing the CCLA's public interest standing.[7]

C. Procedural Background

9. The Applicants commenced this application on May 13, 2014.[8] Following the release of the SCC's decision in *Spencer*, the Applicants filed an amended notice of application on October 31, 2014.[9] The AGC brought a motion to strike the application, which was dismissed by the Honourable Justice R.F. Goldstein on June 16, 2016.[10]

---

[5] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at paras. 2-4, 7, 44.
[6] Affidavit of Michael Geist, sworn May 1, 2015 ["Geist Affidavit"], CCLA Record, Vol. 2, Tab 5 at paras. 2-5.
[7] Affidavit of Sukanya Pillay sworn May 1, 2015 ["Pillay Affidavit"], CCLA Record, Vol. 1, Tab 3.
[8] CCLA Record, Vol. 1, Tab 2.
[9] CCLA Record, Vol. 1, Tab 1.
[10] *Canadian Civil Liberties Association v. Canada*, 2016 ONSC 4172 ["*CCLA v AGC* (2016)"].

10. The AGC delivered its responding application record on March 17, 2017, and the Applicants served a reply affidavit on June 2, 2017.[11] Cross-examinations were conducted in 2017.[12] After a motion on undertakings and refusals in August 2019, the AGC provided its responses to undertakings in November 2020.[13] Pursuant to an Order of this Court dated August 30, 2019, the Applicants further amended the notice of application.[14]

11. In March 2022, the OPC tendered an updated affidavit.[15] In April 2022, the AGC also tendered a further affidavit. In June 2023, the Applicants tendered a supplementary affidavit responding to the undertakings and the new affidavits filed by the AGC and OPC. Cross-examinations on these affidavits took place in October and December of 2023.[16]

D. Legislative Framework

12. *PIPEDA* regulates the collection, use, and disclosure of personal information by private organizations in the course of commercial activity. Part I of *PIPEDA* deals with the protection of personal information in the private sector. Part I must be read in conjunction

[11] Affidavit of Christopher Parsons affirmed June 2, 2017 ["Parsons 2nd Affidavit"], SAR, Tab 2.

[12] Cross-examination transcript of Barbara Dundas, June 21, 2017 ["Dundas Cross-exam"]; Cross-examination transcript of Bruce Wallace, June 21, 2017 ["Wallace Cross-exam"]; Cross-examination transcript of Michael De Santis, June 21, 2017 ["De Santis Cross-exam"]; Cross-examination transcript of Christopher Parsons, June 22, 2017 ["Parsons Cross-exam 2017"]; Cross-examination of Michael Geist, June 22, 2017 ["Geist Cross-exam"].

[13] *Canadian Civil Liberties Association v. Canada*, Order of Belobaba J. dated August 30, 2019, CV-14-504139 (ON SC), SAR, Tab 8.

[14] Further Amended Notice of Application, December 19, 2023, SAR, Tab 1.

[15] Affidavit of Trevor Yeo, dated March 10, 2022, which was "intended to replace the affidavit affirmed by Patricia Kosseim on November 23, 2017" (at para. 2); SAR, Tab 3.

[16] Cross-examination transcript of Trevor Yeo, October 27, 2023 ["Yeo Cross-exam"]; Cross-examination transcript of Christopher Parsons, December 15, 2023 ["Parsons Cross-exam 2023"].

with Schedule 1, which sets out the fair information practices that organizations are required to follow when they manage personal information.

13. The purpose of Part I of *PIPEDA* is two-fold: first, to recognize and protect the right of privacy of individuals with respect to their personal information; and second, to recognize the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate.[17]

14. *PIPEDA* regulates "personal information", which is broadly defined in s. 2(1) as "information about an identifiable individual". *PIPEDA* establishes rules for the (i) collection, (ii) use and (iii) disclosure of personal information by an organization. This application is specifically concerned with the disclosure of personal information.

15. An organization must obtain consent from an individual to disclose their personal information, unless the disclosure falls within an exception created by *PIPEDA*.[18] Under *PIPEDA*, upon request by an individual, an organization must also inform that individual when their personal information has been collected, used or disclosed, unless such notification is prohibited by *PIPEDA*.[19]

---

[17] The purpose of Part I is set out in section 3 of *PIPEDA*: "3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances."

[18] *Wansink v. TELUS Communications Inc*, 2007 FCA 21, at paras. 20-23; Section 6.1 of *PIPEDA;* Clause 4.3 of Schedule 1 (also referred to as "Principle 3 – Consent") stipulates that "[t]he knowledge and consent of the individual are required for the collection, use or disclosure of personal information […]". Section 5(1) requires that every organization comply with the obligations set out in Schedule 1, subject to certain exceptions detailed in sections 6 to 9.

[19] Clause 4.9 of Schedule 1 (also referred to as "Principle 9 – Individual Access") stipulates that "[u]pon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information."

E. The Impugned Provisions

16. Section 7(3)(c.1) creates an exception to the usual requirement that an organization obtain the consent of an individual prior to disclosing their personal information. Section 7(3)(c.1) permits an organization to disclose personal information to a "government institution" without the individual's knowledge or consent if the government institution has identified its "lawful authority to obtain the information", and made the request in one of the four circumstances enumerated in subsections (c.1)(i)-(iv), which generally relate to national security and law enforcement:

> **Disclosure without knowledge or consent**
>
> **(3)** For the purpose of clause 4.3 of Schedule 1… an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is…
>
> **(c.1)** made to a government institution…that has made a request for the information, identified its lawful authority to obtain the information and indicated that
>
> > **(i)** it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
> >
> > **(ii)** the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,
> >
> > **(iii)** the disclosure is requested for the purpose of administering any law of Canada or a province, or
> >
> > **(iv)** the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual

17. Sections 9(2.1), 9(2.2), 9(2.3) and 9(2.4) (the "Veto Provisions") limit what an individual can learn about disclosure requests that are made by government institutions. They enable a government institution to prohibit a private organization from notifying an individual that their personal information has been disclosed to a government institution under subparagraphs 7(3)(c.1)(i) or (ii).

18. The Veto Provisions operate as follows. At any time, an individual may ask a private organization (e.g., a TSP) whether it has disclosed their personal information to a government institution. If the organization has disclosed such information under s.7(3)(c.1)(i) or (ii), then it must notify the relevant government institution of the individual's request for disclosure. The organization must then wait, before complying with the request, until either the institution responds or a specified period of time has passed.[20]

19. The government institution may respond and prohibit the organization from complying with the individual's request on the grounds that "compliance with the request could reasonably be expected to be injurious to" certain specified grounds set out in s.9(2.3).[21] The organization, if prohibited from complying with an individual's request, must refuse to provide the individual with any information and must notify the Commissioner of this refusal under s.9(2.4).[22]

20. The Commissioner is not compelled by statute to do anything with these notifications. Moreover, when receiving a report under s.9(2.4)(b) or otherwise, the Commissioner has no power to investigate government institutions and ensure that their use of their veto power is in compliance with *PIPEDA*. *PIPEDA*'s investigation and enforcement regime is focused on the private organizations only, and so while the OPC has general powers to review an organization's compliance with *PIPEDA*, there is no

[20] *PIPEDA*, s. 9(2.1) and 9(2.2).

[21] These are: "(a) national security, the defence of Canada or the conduct of international affairs; (a.1) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or (b) the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law": *PIPEDA*, s. 9(2.3).

[22] *PIPEDA*, s. 9(2.4).

mechanism for the OPC to assess whether government institutions are appropriately asserting the exceptions encoded in 9(2.3).[23]

F. Basic Subscriber Information

21. This application is concerned with the disclosure of subscriber information, including basic subscriber information. The SCC found such information in *Spencer* and in *R. v Bykovets* ("*Bykovets*") to be subject to a reasonable expectation of privacy because such information might link an individual to a highly detailed profile of online activity.[24]

22. Basic subscriber information is not a defined term in *PIPEDA*, and is a "contested term".[25] It may include a wide range of information from name and address to email address, IP address, billing information, and digital identifiers that link subscriber information to a particular device[26] and cell phone and other digital identifiers.[27] In *Spencer*, the SCC determined that a reasonable expectation of privacy attaches to subscriber information associated with an individual IP address and that s.7(3)(c.1)(ii) does not diminish that reasonable expectation of privacy.[28] In *Bykovets*, the SCC determined that a reasonable expectation of privacy attaches to the IP address itself.[29]

23. As the SCC recognized in *Bykovets*, the "internet has exponentially increased both the quality and quantity of information stored about Internet users, spanning the most

---

[23] *PIPEDA*, ss. 11, 12, 13, 14 and 18. Sections 11(1), 11(2), and 13 outline investigations findings into "organizations" and their compliance with *PIPEDA*, not into government institutions. Section 14 likewise provides a trial de novo tied to the subject matter of the complaint itself. Audits under s. 18 are similarly limited to the "management practices of an organization", not of the government institution.

[24] *Spencer* at para. 66; *R. v. Bykovets*, 2024 SCC 6 at paras. 74-78 ["*Bykovets*"].

[25] Parsons Cross-exam 2017, at pp. 140-141, Q. 538.

[26] Geist Cross-exam, at pp. 12-13, Q. 41-43.

[27] Parsons Cross-exam, at p. 141, Q. 538.

[28] *Spencer* at para. 52.

[29] *Bykovets* at para. 28.

public and the most private human behaviour". The nature of the information that this basic subscriber information may betray, then, is intensely private. Information once revealed to the state in pieces can now be "compiled, dissected and analyzed to lend new insights into who we are as individuals or populations".[30] Aggregation is the key; aggregated data "can reveal new facts about a person that they did not expect would be known when the original, isolated data was collected". Even "information that may at first blush appear mundane and outside of the biographical core may be profoundly revealing when situated in context with other data points".[31]

G. TSPs' Disclosure of Information

24. This application is concerned specifically with the disclosure by TSPs. However, as the SCC recognized in *Bykovets*, in internet age, a range of third-party organizations mediate the privacy relationship between the government and individuals.[32] The Impugned Provisions permit a broad scope of voluntary cooperation with Canadian and foreign law enforcement by a range of third-party private service providers, including and not limited to TSPs, online payment processing entities (like Moneris or Paypal), banks, social media sites, email providers, and airlines (subject to *Charter* constraints).

25. TSPs in particular continue to disclose personal information at high levels. Government institutions, including the six agencies listed above, have in the past sought disclosure of personal information from Canadian TSPs on a massive scale.[33] In 2011

[30] *Bykovets* at para. 73.
[31] *Bykovets* at para. 74.
[32] *Bykovets* at para. 78.
[33] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at paras. 26-35, 37-38.

alone, government institutions made approximately one million requests of TSPs.[34] A significant majority of these disclosures were made without prior judicial authorization.[35]

26. Government institutions seek and obtain disclosure of personal information from TSPs for a variety of purposes. The information that is collected by government institutions pursuant to section 7(3)(c.1) of *PIPEDA* may be used in connection with criminal charges and proceedings, and for national security and intelligence-gathering purposes. The information can be shared with other domestic agencies, and also with foreign agencies in connection with matters of national security, international affairs or for purposes of law enforcement in a foreign jurisdiction.[36]

27. It is the Applicants' position that *PIPEDA* does not provide adequate accountability mechanisms or safeguards to ensure that government institutions have lawful authority to make requests pursuant to section 7(3)(c.1), and places private corporations in the position of having to assess whether government institutions have lawful authority, or whether there are "exigent circumstances" that may obviate the need for a warrant.[37]

28. Some TSPs in Canada publish "transparency reports" that give aggregate information on the number of disclosure requests that are made and fulfilled. However, publication of these reports and the content therein are not mandatory.[38] The guidelines promulgated by Industry Canada for the publication of such reports are non-compulsory, and the transparency reports that are published by Canadian TSPs vary significantly, both

---

[34] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at para. 37.
[35] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at para. 31.
[36] *Wakeling*, dissent of Karakatsanis J. at paras. 118-120.
[37] Affidavit of Christopher Parsons, affirmed May 3, 2023 ["Parsons 3rd Affidavit"], SAR, Tab 4 at para. 3.
[38] Parsons 3rd Affidavit, SAR, Tab 4 at para. 3.

in form and content[39] or are often drafted to accord with the TSPs own commercial interests and goals and to minimize any efforts to require notifying individuals of government requests for their personal information.[40] This is concerning in the context of the evidence that government agencies do not systematically keep track of access requests for basic subscriber information, and so appear to rely entirely on private sector transparency reports to monitor such requests.[41]

H. Lawful Authority

29. The requirement in s.7(3)(c.1) that a government institution identify its "lawful authority" to obtain requested information has been applied inconsistently since *Spencer.*

30. A government institution conducting a search for personal information protected by *PIPEDA* cannot simply make a "bare request" for the information; the institution must identify a source of authority not found within *PIPEDA*. However, the scope of what constitutes lawful authority remains broadly construed and ill-defined. *Spencer* confirmed that *PIPEDA* is not, itself, a source of lawful authority; s.7(3)(c.1)(ii) is not an authorizing law within the meaning of s.8 of the *Charter,* and does not authorize a search or seizure absent some other lawful authority, such as a reasonable law or exigent circumstances.[42] However, the SCC noted that "lawful authority" under s.7(3)(c.1) to obtain personal information "may include several things", including "the authority of police to conduct

[39] Parsons 3rd Affidavit, SAR, Tab 4 at para. 3.
[40] Parsons 3rd Affidavit, SAR, Tab 4 at para. 24.
[41] Parsons 3rd Affidavit, SAR, Tab 4 at para. 11.
[42] *Spencer* at para. 71-73.

warrantless searches under exigent circumstances or where authorized by a reasonable law".[43] Lawful access may refer to either warrantless or warranted access.[44]

31. On the evidence, there are instances where physical or digital "*PIPEDA* letters"—i.e., a letter issued by law enforcement to TSPs in order to gain access to basic subscriber data—have been issued with bare assertions of lawful authority, without a warrant, including requests for information that inappropriately relied on s.7(3)(c.1)(2) as an independent source of lawful authority.[45] These *PIPEDA* letters demonstrate that law enforcement agencies, without judicial oversight but by asserting their lawful authority, are requesting warrantless access to subscriber data.

32. The AGC argues that there are many laws upon which a government institution may rely to request personal information from an organization. The AGC argued on its motion to strike that it could not respond to the application because there were too many possible sources of lawful authority, with varying accountability regimes. However, the AGC has failed to provide any evidence about such laws or their accountability regimes.

33. By way of illustration, under its governing legislation, CSIS shall:

(a) "collect, by investigation or otherwise […] and analyse and retain information and intelligence respecting activities that may on reasonable grounds be suspected of constituting threats to the security of Canada";[46]

---

[43] *Spencer* at para. 71.
[44] Parsons Cross-exam 2017, at pp. 57-58, Q. 195-197.
[45] Parsons Cross-exam 2017, at pp. 50-54, Q. 165-180.
[46] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23, s. 12(1) ["*CSIS Act*"].

(b) "in relation to the defence of Canada or the conduct of the international affairs of Canada, assist…in the collection of information or intelligence relating to the capabilities, intentions or activities" of "any foreign state or group of foreign states" or any person other than a Canadian citizen or non-permanent resident.[47]

34. As a result of the Court's direction in *Spencer*, a private entity subject to *PIPEDA* may face a request to disclose information to CSIS in circumstances covered by these provisions. While s. 7(3)(c.1)(ii) of *PIPEDA* prohibits the entity subject to *PIPEDA* (i.e., TSPs) from voluntarily disclosing personal information absent a request accompanied by lawful authority, nothing in *PIPEDA* ensures that government assertions of lawful authority would withstand judicial scrutiny. There is no mechanism by which a TSP may verify the government's asserted lawful authority underlying its information request, and certainly not one by which the TSP can confirm exigent circumstances exist. Further, on the evidence, it will be up to the TSP to determine whether these criteria have been met. TSPs range from major corporations with large compliance departments (though there is no reason to expect them to have any particular expertise in constitutional doctrine) to small operations that rely on one or two people to process disclosure requests.[48] Whether or not privacy breaches will occur will effectively be determined by private corporations of varying resources and skillsets—none of which have any particular incentive to challenge the authority of government requests.

[47] *CSIS Act,* s. 16(1).
[48] Parsons 2nd Affidavit, SAR, Tab 2 at para. 13.

35. In practice, this may allow government institutions to push the boundaries of exigent circumstances or what lawful authority allows.[49] In its responses to undertakings ordered by Belobaba J. on the refusals motion brought by the Applicants, the AGC advises that neither of the RCMP or CBSA tracks the information required to know how many voluntary disclosures were made by TSPs at the request of a government organization or on the initiative of the organization, or what disclosures were made in emergency or exigent circumstances or in compliance with federal or provincial law. (The responses of both CSIS and CSE were that each was not able to respond to this question in an open forum).[50]

36. When law enforcement agencies request basic subscriber information but lack a production order, exigent circumstances, or other legislative authorization, disclosing that subscriber information without consent would place a TSP in violation of *PIPEDA*. However, keeping in mind the fact that individuals are generally unaware of and would have no reason to ask about disclosures, the recalcitrance of TSPs to provide information transparently even if they are asked,[51] and the ability of agencies to prohibit disclosure with no effective supervision under the Veto Provisions, it is almost inevitable that TSPs will disclose basic subscriber information in situations where law enforcement agencies are 'pushing the envelope' and asserting lawful authority that a court might conclude does

[49] See, for example, CSIS attempts to access subscriber data in *Re X*, 2017 FC 1048; see also the Court's comments with respect to the conflating of access requests in Canadian Security Intelligence Services Act (RE), 2020 FC 697 at 75.

[50] AGC's Responses to Undertakings and Refusals, November 18, 2020, SAR, Tab 5 at Appendix A.

[51] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at paras. 44-52. If an expert in the field is left confused and unenlightened by his own TSP's responses to his requests for information, it seems likely that average requesters will obtain little or no useful information from their own inquiries.

not actually exist. In the absence of accountability and transparency mechanisms, there is nothing to prevent the privacy interests of people in Canada from being infringed.

I. An Individual's Knowledge of an Information Request

37. TSPs will generally not advise affected individuals that their information has been the subject of a request or disclosure.[52] As noted above, while an individual may request that a TSP inform them about any disclosure of information to a government institution,[53] that institution can prevent the TSP from informing the individual about such disclosure,[54] giving government institutions a veto over the release of this information.[55]

38. Without knowing who is collecting personal data, for what purpose, for how long, or the grounds under which they share it, on a practical level an individual can neither exercise their rights nor evaluate whether an organization is appropriately handling their data. In an apparent attempt to address this, *PIPEDA* empowers individuals to issue legally-binding Data Access Requests ("DARs") to private companies to answer exactly these kinds of questions.[56] However, TSPs do not generally provide detailed records in response to requests for DARs, including with respect to requests for call logs, cell tower connections, and other metadata. Some companies informed requesters that they could provide records for a fee if the requester specified a date range, and companies tended to not offer requesters a sample set of records prior to receiving a fee.[57]

---

[52] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at paras. 30, 38.
[53] *PIPEDA*, s. 9(2.1)(a)(i).
[54] *PIPEDA*, ss. 9(2.2) – (2.4).
[55] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at para. 42.
[56] Parsons 3rd Affidavit, SAR, Tab 4 at para. 16.
[57] Parsons 3rd Affidavit, SAR, Tab 4 at paras. 19-20.

39. This is of particular concern because the only real accountability mechanism built into *PIPEDA* places the onus on individuals, who may not know that their information has been disclosed, to initiate a review of an organization's compliance with *PIPEDA*.[58] The Commissioner's and OPC's oversight of compliance with *PIPEDA* in this respect is driven by whether they receive individual complaints.[59] Between 2012 to 2023, there were only 3910 complaints accepted by the OPC.[60] Apart from individual decisions[61], there is no general audit that the OPC was aware of to ensure whether organizations were following their s. 9(2.4)(b) obligations.[62]

40. The AGC's own evidence was that even in situations where a government institution (in this case, the RCMP) holds subscriber data for a specified period under privacy regulations, and the individual has the right to request that information during that time period, they did not know how an individual would find out that the government institution had requested that information.[63] As a result, absent criminal proceedings in which disclosure obligations apply, government requests for personal information from TSPs or other organizations governed by *PIPEDA* may never come to light.[64]

---

[58] *PIPEDA*, s. 11-17.

[59] Yeo Cross-exam, at pp. 9-11, Q. 20-28.

[60] Privacy Commissioner of Canada's Answers to Advisements and Undertakings, November 30, 2023, SAR, Tab 6 at Appendix 1.

[61] See e.g. the Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2016-008 <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-008/>

[62] Yeo Cross-exam, at pp. 34-35, Q. 108-110.

[63] Dundas cross-exam, at p. 15, Q. 48.

[64] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4, at para. 51; Geist Affidavit, CCLA Record Vol. 2, Tab 5, at para. 18.

J. Information Collected Pre-Spencer

41. On cross-examination in 2017, the AGC's witnesses confirmed that there is no legislative or statutory limit after which basic subscriber information is destroyed.[65] In late 2020, in responses to undertakings, the AGC confirmed that there is no government initiative following *Spencer* to destroy basic subscriber information collected from telecommunications service providers prior to release of *Spencer*. There remains as of 2023 no initiative to destroy basic subscriber information collected prior to the release of *Spencer* at the RCMP, CSIS, CSE, CBSA, CRA or Competition Bureau.[66]

PART III. ISSUES

42. This application raises the following issues:

(a) Do the Impugned Provisions violate the right to be free from unreasonable search and seizure under s.8 of the *Charter*?

(b) Do the Impugned Provisions violate the right to liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice under s.7 of the *Charter*?

(c) Do the Impugned Provisions violate the right to free expression under s. 2(b) of the Charter?

(d) If the Impugned Provisions violate s.8 or s. 2(b) of the *Charter,* is the violation saved by s.1 of the *Charter*?

(e) If the violation is not saved by s.1, what is the appropriate remedy?

---

[65] Dundas cross-exam, at p. 16, Q. 52.

[66] Parsons 3rd Affidavit, SAR, Tab 4 at paras. 22, 32-34.

PART IV. LAW AND ANALYSIS

A. The Applicants' Standing

43. The Applicants bring this application as public interest litigants. To date, the AGC has not challenged their standing.[67] The CCLA has long been acknowledged as a leading voice for civil liberties in Canada, including privacy rights and freedom of expression.[68] It is well established that public interest standing may be recognized where a credible organization raises serious legal issues as to the validity of legislation, has shown a genuine interest in the subject matter, and puts forward a reasonable manner of challenging laws that may otherwise go unchallenged.[69] These factors must be applied in a "flexible and generous manner" in light of the underlying policy rationales.[70] The Applicants defer any further comment on standing to their reply, in the event that their standing is contested.

B. The Impugned Provisions Violate Section 8

1. Overview of Section 8

44. Section 8 of the *Charter* guarantees all individuals "the right to be secure against unreasonable search or seizure."[71] The Impugned Provisions violate s.8 of the *Charter.* Privacy is a core concern of s. 8. The collection of basic subscriber information by government agencies violates the individual's reasonable expectation of privacy.

---

[67] *CCLA v. AGC* (2016) at para. 11.

[68] Pillay Affidavit, CCLA Record, Vol. 1, Tab 3, at paras. 3-4.

[69] *Downtown Eastside Sexworkers United Against Violence Society v Canada (Attorney General)*, 2012 SCC 45 ["*Downtown Eastside*"]; *British Columbia (Attorney General) v. Council of Canadians with Disabilities*, 2022 SCC 27. This is particularly true in the case of a broad and systemic challenge to a legislative scheme, such as the present case: *Downtown Eastside*, para. 73.

[70] *Downtown Eastside* at para. 20.

[71] *The Constitution Act, 1982*, Schedule B to the *Canada Act 1982* (UK), 1982, c 11, at s. 8.

45. As noted by the SCC in *Bykovets*, "[a]nonymity is a particularly important conception of privacy when it comes to the Internet".[72] The privacy interest affected by government requests for basic subscriber data is informational privacy. Informational privacy protects the right of "individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[73] Information that is at the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state" is subject to a high expectation of privacy.[74] Information that "tends to reveal intimate details of the lifestyle and personal choices of the individual" falls within the "biographical core", and is protected by s.8.[75]

46. The internet and digital technology are increasingly integral to daily life, and people should be able to reasonably expect that the data points generated by their activities and devices online will remain free from state search and seizure.

2. Basic Subscriber Information and a Reasonable Expectation of Privacy

47. There is a reasonable expectation of privacy in basic subscriber information and access to that information absent lawful authority constitutes a search.

48. A search occurs where an individual has a reasonable expectation of privacy, measured both subjectively and objectively, in the subject matter of the alleged search or

---

[72] *Bykovets* at para. 46.
[73] *R v Tessling*, 2004 SCC 67 at para. 23 ["*Tessling*"].
[74] *R v Plant,* [1993] 3 SCR 281 ["*Plant*"] at p. 293.
[75] *Plant* at p. 293.

seizure.[76] In this way, the guarantee of security from unreasonable search is fundamentally an entitlement to a reasonable expectation of privacy.[77]

49. Basic subscriber data is deeply personal in nature. As the SCC recognized in *Spencer* and *Bykovets*, subscriber information links particular kinds of information to identifiable individuals, and gives rise to a privacy interest.[78] The privacy interest is grounded in the notion of privacy as anonymity—namely, that there is an interest in protecting the identity of the person associated with particular information.[79] This understanding of privacy is especially relevant in the context of using the Internet.[80] As the SCC noted in *Bykovets*:[81]

> A great deal of online activity is performed anonymously (*Spencer*, at para. 48; *Ward*, at para. 75). People behave differently online than they do in person (*Ramelson*, at para. 5). "Some online locations, like search engines, allow people to explore notions that they would be loath to air in public; others, like some forms of social media, allow users to dissimulate behind veneers of their choosing" (para. 46). We would not want the social media profiles we linger on to become the knowledge of the state. Nor would we want the intimately private version of ourselves revealed by the collection of key terms we have recently entered into a search engine to spill over into the offline world. Those who use the Internet should be entitled to expect that the state does not access this information without a proper constitutional basis.

50. The Internet has dramatically expanded the amount and detail of information collected about its users, and individuals often lack both control over and awareness of who may be tracking their online behavior. The volume of data available about a user and the connections that can be drawn by an aggregation of those data points are substantial. As a result, maintaining anonymity is one of the few ways users can reasonably expect

---

[76] *Tessling* at para. 32; *R. v. Ward,* 2012 ONCA 660, at para. 86.
[77] *Hunter et al v Southam Inc*, [1984] 2 SCR 145 ["*Southam*"] at pp. 159-160.
[78] *Spencer* at para. 47.
[79] *Spencer* at paras. 42, 47-48.
[80] *Spencer* at paras. 41-43.
[81] *Bykovets* at para. 67.

their online activities to remain private.[82] Merely comparing the IP address of an identified user with other online activities "shatters [online] anonymity completely".[83]

3. The disclosure regime in *PIPEDA* is not reasonable

51. If an individual has a reasonable expectation of privacy in the subject matter of the state's investigation, then s.8 is engaged and the search of that subject matter by a government authority must be reasonable. The disclosure regime created by *PIPEDA* must be reasonable to comply with s.8 of the *Charter*.[84] The disclosure regime created by *PIPEDA* does not satisfy s. 8 because the scheme, as a whole, fails to provide meaningful oversight over the disclosure of personal information.

52. Meaningful oversight is an essential constitutional check on state intrusion into personal privacy.[85] The SCC in *R v. Tse* ("*Tse*") held that the emergency wiretap provisions in the *Criminal Code* were unconstitutional for want of meaningful oversight:

> [84] The jurisprudence is clear that an important objective of the prior authorization requirement is to prevent unreasonable searches. In those exceptional cases in which prior authorization is not essential to a reasonable search, additional safeguards may be necessary, in order to help ensure that the extraordinary power is not being abused. Challenges to the authorizations at trial provide some safeguards, but are not adequate as they will only address instances in which charges are laid and pursued to trial. Thus, the notice requirement, which is practical in these circumstances, provides some additional transparency and serves as a further check that the extraordinary power is not being abused.
>
> [85] In our view, Parliament has failed to provide adequate safeguards to address the issue of accountability in relation to s. 184.4. Unless a criminal prosecution results, the targets of the wiretapping may never learn of the interceptions and will be unable to challenge police use of this power. There is no other measure in the Code to ensure specific oversight of the use of s. 184.4. For s. 8 purposes, bearing in mind that s. 184.4 allows for the highly intrusive interception of private

---

[82] *Spencer* at para. 46. See also *R. v. Otto*, 2019 ONSC 2473; *R. v. Mohamed and Ali*, 2021 ONSC 2790; *R. v. Marakah*, 2022 ONSC 4867; and *R. v. Benstead*, 2025 MBPC 8.

[83] *Bykovets* at para. 80.

[84] *Wakeling v United States of America,* 2014 SCC 72 ["*Wakeling*"] at paras. 37-38; and *Goodwin v British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46 ["*Goodwin*"] at para. 71.

[85] *R v Tse*, 2012 SCC 16 [*"Tse*"] at paras. 11, 84-85. See also *Goodwin* at paras. 70-71; *Southam* at p. 169.

> communications without prior judicial authorization, we see that as a fatal defect. In its present form, the provision fails to meet the minimum constitutional standards of s. 8 of the Charter.[86]

53. Similarly, the Impugned Provisions in *PIPEDA* have no oversight mechanism. An oversight mechanism is critical for constitutionality.

54. The SCC held in *Tse* that the absence of a statutory requirement for after-the-fact notice to individuals whose information had been disclosed violated the minimum constitutional standards required under s.8 of the *Charter*.[87] Moreover, the SCC found that individual s.8 challenges in criminal proceedings arising from searches or seizures pursuant to emergency wiretap provisions were not sufficient to remedy the breach.[88]

55. *PIPEDA* also has no after-the-fact notice requirement. Indeed, individuals whose information has been shared with government institutions pursuant to the Impugned Provisions may never learn of the disclosure, unless it is revealed in a subsequent criminal prosecution. In this way, *PIPEDA*'s disclosure scheme does not meet the minimum constitutional requirements under s.8.

56. *PIPEDA* does not provide for any mandatory reporting in respect of information requests made to private organizations pursuant to s.7(3)(c.1). Reporting requirements, either to a judicial body or parliament, form an important part of meaningful oversight within the meaning of s. 8.[89] The absence of any reporting requirement is constitutionally

---

[86] *Tse* at paras. 83-84.
[87] *Tse* at paras. 11 and 85.
[88] *Tse* at paras. 84-85.
[89] *Wakeling* at para. 66; *Tse* at paras. 87-90.

deficient. Moreover, the existence of the Veto Provisions actively undermines the opportunity for notification to individuals.

57. Finally, *PIPEDA* contains no limits or oversight on a government institution's subsequent use of personal information. Many government institutions can and do use acquired personal information for a variety of national security purposes, and share such information with other domestic and foreign agencies.[90] When a government agency has shared information with a foreign jurisdiction, Canada effectively loses control over the information, its use, dissemination and further disclosure. As Karakatsanis J. stated in her dissent in *Wakeling*, "[w]hen information is shared across jurisdictional lines, the safeguards that apply in domestic investigations lose their force. This can create serious risks to individual privacy, liberty and security of the person interests."[91] The *PIPEDA* disclosure scheme does not meet the minimum standards required by s.8, which demands limits and oversight on the subsequent disclosure of personal information acquired by a search or seizure.[92]

58. Whether an expectation of privacy is reasonable depends on the "totality of the circumstances", including the nature of the information at stake.[93] The applicants recognize that defining a reasonable expectation of privacy is an exercise in balance between privacy and protection.[94] The AGC may argue that the powers in s. 7(3)(c.1)

---

[90] *Wakeling*, dissent of Karakatsanis J. at paras. 118-120.
[91] *Wakeling*, dissent of Karakatsanis J. at para. 118.
[92] *Goodwin* at para. 71: the SCC in *Goodwin* held that oversight for s. 8 is extended beyond just the search, to also include "the use and reliability of its findings". See also *Wakeling*, dissent of Karakatsanis J. at para. 118.
[93] *Spencer* at para. 34; *Bykovets* at para. 45.
[94] *Tessling*, at para. 17; *Bykovets* at para. 71.

relate to matters of law enforcement or national security only, and that these goals provide an adequate counterweight to the privacy rights held by individuals. However, these goals writ large are not sufficient to justify the ongoing infringement into privacy rights by the Impugned Provisions. Without meaningful safeguards as a substitute for prior judicial authorization, searches conducted through ss. 7(3)(c.1) of *PIPEDA* fall far short of s.8's minimum constitutional requirements. Where a reasonable expectation of privacy exists, a warrantless search is presumptively unreasonable. A warrantless search will be unreasonable unless it is authorized by a reasonable law and carried out in a reasonable manner.[95]

C. The Impugned Provisions Violate Section 7

1. The Provisions Violate the Right to Liberty and Security of the Person

59. The Impugned Provisions also violate s. 7. The SCC has accepted that s. 7 provides residual protection for privacy interests and that privacy can be a protected component of the liberty and security of the person interests.[96] State-induced disclosure of a person's intimate personal information may infringe this s.7 right.[97]

60. To establish a violation of s. 7, an applicant must prove, on a balance of probabilities, that the state action:

---

[95] *R v Collins,* [1987] 1 SCR 265 at paras. 22-23.

[96] *R. v. Mills*, [1999] 3 S.C.R. 668, and especially at paragraphs 77-89, 94, 99 and 108, where the court embedded privacy analysis based on section 8 considerations within analysis of a section 7 principle of fundamental justice; *R. v. O'Connor*, [1995] 4 S.C.R. 411 ["*O'Connor*"], at paragraphs 110-119; *B.(R.) v. Children's Aid Society of Metropolitan Toronto*, [1995] 1 S.C.R. 315, at page 369; *R. v. Beare*, [1988] 2 S.C.R. 387 at para 58; see also *Cheskes v. Ontario (Attorney General)* (2007), 2007 CanLII 38387 (ONSC) ["*Cheskes*"].

[97] *O'Connor* at paras. 110-119; *R. v. Mills*, 1999 CanLII 637 (SCC) at paras. 79-85; *Husky Oil Operations Limited v. Canada-Newfoundland and Labrador Offshore Petroleum Board*, 2018 FCA 10 at para. 23; *Cheskes* at paras. 78-85; *Catholic Children's Aid Society of Hamilton v. L.K.*, 2016 CanLII 15148 (ON SC) at para. 11.

(a) deprives, in the sense that it limits, negatively impacts, or interferes with, life, liberty or security of the person, or creates a risk of such deprivation;

(b) is causally connected with that increased risk; and

(c) increases the applicant's risk of harm in a way that does not accord with the principles of fundamental justice, in that it is arbitrary, overbroad, or grossly disproportionate. [98]

61. All three requirements are met in this case. Basic subscriber information linked to information such as location history, contact networks, and patterns of communication, can reveal significant information about a person. It can be used to identify otherwise anonymous metadata obtained by various means, and it can also be used to identify anonymous online content obtained by various means. In so doing, it can identify and reveal intimate details about an individual's life—religious affiliations, political beliefs, sexual orientations, health concerns, or personal relationships. This limits or negatively impacts the liberty or security of that person.

62. The deprivation caused by the mechanism in *PIPEDA* which allows the state to obtain basic subscriber information from TSPs increases an individual's risk of harm to their liberty and security of the person interests. Respect for individual privacy is an essential component of what it means to be "free". As a corollary, the infringement of this right undeniably impinges upon an individual's "liberty" in our free and democratic society.[99]

---

[98] *Canadian Council for Refugees v. Canada*, 2023 SCC 17 at para. 56; *Canada (Attorney General) v. Bedford*, 2013 SCC 72, at paras. 75 ["*Bedford*"].

[99] *Cheskes*, at paras. 78-85.

2. The Violation of the Right to Liberty and Security of the Person Is Not in Accordance with the Principles of Fundamental Justice

(a) Absence of Accountability Mechanisms

63. The legislative scheme interferes with liberty and security of the person in a manner that is not in accordance with the principles of fundamental justice. In addition to the lack of accountability outlined above, the Veto Provisions, which effectively provide the state agency requesting personal information with a veto over whether the subject of that information is ever informed of disclosure pursuant to s.7(3)(c.1), violate s. 7 of the *Charter* by failing to protect individuals from intrusive state-induced disclosure of sensitive personal information. It is fundamentally unjust that individuals can have their informational liberty and security of the person interests infringed without any oversight mechanism.

(b) Vagueness, Arbitrariness and Overbreadth

64. Moreover, an interrelated contravention of the principles of fundamental justice arises from the vagueness of s. 7(3)(c.1), as interpreted post-*Spencer*. That provision, coupled with its subsequent judicial interpretation, does not provide individuals or organizations subject to *PIPEDA* with meaningful guidance about the circumstances in which it can be applied. As such, it is unconstitutionally vague. Lack of accountability was found to be a fatal constitutional defect for warrantless wiretap provisions in *Tse*. The Applicants submit that this logic applies to both s.7 and s.8 of the *Charter*. Vagueness has been recognized as a principle of fundamental justice by the SCC.[100]

[100] *Reference re ss. 193 and 195.1(1)(c) of the Criminal Code (Man.)*, [1990] 1 SCR 1123 at p. 1156.

65. The SCC in *Spencer* held that the "lawful authority" referenced in the Impugned Provisions of *PIPEDA* may include:

(a) the common law authority of the police to ask questions relating to matters that are not subject to a reasonable expectation of privacy; and

(b) the authority to conduct warrantless searches under exigent circumstances or where authorized by a reasonable law.[101]

66. A private entity subject to *PIPEDA* is expected to disclose information to a government agency that requests it and cites its lawful authority to collect it. It is then up to the entity subject to *PIPEDA* to determine whether these criteria have been met. The SCC's decision in *Spencer* highlights the multi-faceted nature of privacy, and acknowledges (as noted above) that determining whether a reasonable expectation of privacy exists is based on the totality of the circumstances.[102] If the *PIPEDA* scheme leaves this determination to the entity that has collected the information (a TSP, for example), individuals have no way of knowing when information may be disclosed. Indeed, there are no criteria that can be applied consistently by the broad range of entities that are subject to *PIPEDA*.

67. In *Tse,* the emergency wiretap provisions at issue were challenged under both s.7 and s.8, but the Court did not find a breach of s.7 because it found that the conditions restricting the use of the power were sufficiently strict to avoid a conclusion that they were impermissibly vague or overbroad.[103] However, no such determination has been made

[101] *Spencer* at para. 71.
[102] *Spencer* at para. 17.
[103] *Tse* at paras. 9, 29-59.

with respect to the Impugned Provisions of *PIPEDA*. One issue on which the SCC expressed concern in *Tse* was the wide range of people who might have access to the wiretap provisions under the definition of "peace officer".[104]

68. For similar reasons, the legislative scheme is arbitrary and overbroad, contrary to the principles of fundamental justice. If there are no real standards, no transparency, no oversight mechanisms, and no institutional structures to confine disclosure requests to those that might be justified as reasonable, then the results will be arbitrary and not connected to the legitimate purposes of the legislative scheme. Similarly, the results will likely go well beyond the realm of justifiable disclosure.

D. The Veto Powers Violate s. 2(b)

69. The Veto Provisions violate the right to freedom of expression in s. 2(b). In *Ontario (Public Safety and Security) v. Criminal Lawyers' Association* the SCC held that s. 2(b) includes the right of individuals and organizations to request access to government documents where the denial of access substantially impedes meaningful public discussion and criticism on matters of public interest.[105]

70. *PIPEDA* generally allows individuals to ask organizations whether their personal information has been disclosed to a government institution and for information related to requests and disclosure. However, under the Veto Provisions, the requesting government institution effectively has a veto power over the release of this information. The OPC has a limited ability to oversee or challenge how government institutions assert this veto, and

[104] *Tse* at para. 57.
[105] 2010 SCC 23.

there is no mechanism in *PIPEDA* for an organization to challenge a government's veto regarding disclosure.[106]

71. As a result, there are circumstances under which an individual would have no means of determining whether their personal information has been requested and/or obtained by a government institution. Individuals may never learn about the disclosure of their personal information, and may not know the content of personal information requested by government institutions. A reliance on voluntary disclosure is not adequate.[107]

72. The broad ability to veto, without any ability for verification, oversight or challenge, substantially impedes meaningful public discussion and criticism (indeed, knowledge) about the government's collection of basic subscriber information under the Impugned Provisions. The evidence of Dr. Parsons confirms that there is a significant public interest in obtaining information about these practices.[108]

E. The Impugned Provisions are not saved by s. 1

73. Violations of s. 7 are, in general, "difficult to justify" under s. 1 given the significant overlap between the two sections.[109] Similarly, if the Impugned Provisions authorize

---

[106] Other acts do have such alternative procedural protections; see for example *Ruby v. Canada (Solicitor General)*, 2002 SCC 75 at para. 47.

[107] *ARPA Canada and Patricia Maloney v R.*, 2017 ONSC 3285 at para. 44.

[108] Parsons 1st Affidavit, CCLA Record, Vol. 1, Tab 4 at paras. 45-46. Parsons describes his development of the "Access My Information" App by which members of the public could seek information from their TSPs on disclosure requests, which was viewed by 50,000 to 60,000 visitors to the site, and for which over 1500 individuals opted into the mailing list.

[109] *R. v. Sharma,* 2022 SCC 39, dissent of Karakatsanis J. at para. 253 ["*Sharma*"]; *Bedford* at paras. 124, 129.

unreasonable searches contrary to s.8, they are unlikely to be demonstrably justified as a reasonable limit under s.1.

74. While the government may argue that the objective of requiring secret production under the Impugned Provisions is to protect public safety and assist in law enforcement, this goal, although laudable, cannot automatically justify infringing fundamental privacy rights. The objective must be pressing and substantial. The law must also show a clear causal link between requiring production of basic subscriber information and the achievement of the legislative objective.

75. The Impugned Provisions impair privacy rights more than reasonably necessary. The mandatory production of basic subscriber information coupled with the fact that the government can stop a TSP from advising an individual who requests it that their information has been requested cannot be minimally impairing. The government has failed to demonstrate that less intrusive alternatives—such as obtaining basic subscriber information only with demonstrated lawful authority or limiting data collection to specific cases under judicial supervision—are insufficient to meet the law enforcement goals.

76. Finally, in a balancing of the deleterious effects of the law against its salutary benefits, the negative impact on individuals' privacy, autonomy, and freedom from unwarranted surveillance are profound, particularly given the sensitive and revealing nature of basic subscriber information. This can lead to chilling effects on lawful expression and association, undermining democratic freedoms. In contrast, the benefits of the law—broad informational access—are speculative and marginal at best, especially when obtained without adequate oversight or safeguards.

F. The Appropriate Remedy

77. The Applicants seek declarations of invalidity of the Impugned Provisions. In addition, in the circumstances, the Applicants seek an order that the federal government (or alternatively the six agencies set out above) take steps to delete and destroy the information they have obtained and retained through disclosure requests made under the Impugned Provisions. This is particularly appropriate given the evidence that the federal government made such requests on a massive scale prior to *Spencer*, and has had no process post-*Spencer* to purge information that was unconstitutionally obtained.

78. Where there has been systematic overcollection of personal information contrary to the *Charter*, a systemic remedy is warranted so the government is not rewarded for unconstitutional conduct. In individual cases of breach of privacy rights, it may be sufficient to exclude evidence or provide an alternative individual remedy. Where the breach has occurred in a widespread and systematic manner, however, a broader remedy is called for.

79. In *Re X*,[110] the Federal Court found that CSIS had engaged in unauthorized retention of "associated data" relating to non-targets of investigations that it had no statutory mandate to gather and retain, that it had acquired incidentally in the course of legitimate surveillance of investigation targets pursuant to warrants. "Associated data" consisted of metadata furnished to CSIS from service providers.[111] From 2006, CSIS had an associated data retention program whereby it kept such data indefinitely for use in

[110] *X (Re)*, 2016 FC 1105 ["*Re X*"].
[111] *Re X* at para. 1.

future investigations.[112] The Court held that CSIS was required to destroy such data to the extent that its retention was not statutorily authorized (or seek a statutory amendment), and directed that it do so within a specified time (with provision to seek an extension if required).[113]

80. Directions such as those made in *Re X* would be appropriate in the present case. The stockpiles of basic subscriber information collected prior to *Spencer*, as well as data collected post-*Spencer* to the extent that the Impugned Provisions are invalid, have been collected without proper statutory authority and contrary to the *Charter*. They should not be retained by the federal government.

PART V. ORDER SOUGHT

81. The Applicants therefore seek a declaration that the Impugned Provisions violate s.8, s. 7 and s. 2(b) of the *Charter*, that such violations cannot be saved by s.1 of the *Charter*, and that the Impugned Provisions are therefore of no force or effect. The Applicants further seek an order that the federal government delete and destroy any basic subscriber information that they have obtained in breach of these *Charter* rights.

ALL OF WHICH IS RESPECFULLY SUBMITTED.

Andrew Lokan / Kartiga Thavaraj

Paliare Roland Rosenberg Rothstein LLP
155 Wellington Street West
35th Floor Toronto, ON M5V 3H1
Lawyers for the Applicants

[112] *Re X* at para. 35.
[113] *Re X* at paras. 186-188, 252-253.

SCHEDULE A

1. *R. v. Spencer,* 2014 SCC 43.
2. *Canadian Civil Liberties Association v. Canada,* 2016 ONSC 4172.
3. *Wansink v. TELUS Communications Inc.,* 2007 FCA 21.
4. *R. v. Bykovets,* 2024 SCC 6.
5. *Re X,* 2017 FC 1048.
6. *Canadian Security Intelligence Services Act (RE),* 2020 FC 697.
7. *Downtown Eastside Sexworkers United Against Violence Society v. Canada (Attorney General),* 2012 SCC 45.
8. *British Columbia (Attorney General) v. Council of Canadians with Disabilities,* 2022 SCC 27.
9. *R. v. Tessling,* 2004 SCC 67.
10. *R. v. Plant,* [1993] 3 SCR 281.
11. *R. v. Ward,* 2012 ONCA 660.
12. *Hunter et al. v. Southam Inc.*, [1984] 2 SCR 145.
13. *R. v. Otto*, 2019 ONSC 2473.
14. *R. v. Mohamed and Ali,* 2021 ONSC 2790.
15. *R. v. Marakah,* 2022 ONSC 4867.
16. *R. v. Benstead,* 2025 MBPC 8.
17. *Wakeling v. United States of America,* 2014 SCC 72.
18. *Goodwin v. British Columbia (Superintendent of Motor Vehicles),* 2015 SCC 46.
19. *R. v. Tse,* 2012 SCC 16.
20. *R. v. Collins,* [1987] 1 SCR 265.
21. *R. v. Mills,* 1999 CanLII 637 (SCC).
22. *R. v. O'Connor,* 1995 CanLII 51 (SCC).
23. *B.(R.) v. Children's Aid Society of Metropolitan Toronto,* [1995] 1 S.C.R. 315.
24. *R. v. Beare,* [1988] 2 S.C.R. 387.
25. *Cheskes v. Ontario (Attorney General),* 2007 CanLII 38387 (ON SC).
26. *Husky Oil Operations Limited v. Canada-Newfoundland and Labrador Offshore Petroleum Board,* 2018 FCA 10.
27. *Catholic Children's Aid Society of Hamilton v. L.K.,* 2016 CanLII 15148 (ON SC).
28. *Canadian Council for Refugees v. Canada,* 2023 SCC 17.
29. *Canada (Attorney General) v. Bedford,* 2013 SCC 72.
30. *Reference re ss. 193 and 195.1(1)(c) of the Criminal Code (Man.),* [1990] 1 SCR 1123.
31. *Ontario (Public Safety and Security) v. Criminal Lawyers' Association,* 2010 SCC 23.
32. *Ruby v. Canada (Solicitor General),* 2002 SCC 75.
33. *ARPA Canada and Patricia Maloney v R.,* 2017 ONSC 3285.
34. *R. v. Sharma,* 2022 SCC 39.
35. *X (Re),* 2016 FC 1105.

(a) **SCHEDULE B**

The Constitution Act, 1982

Schedule B to the Canada Act 1982 (UK), 1982, c 11

Fundamental freedoms

2 Everyone has the following fundamental freedoms:

[...]

(b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;

[...]

Life, liberty and security of person

7 Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

Search or seizure

8 Everyone has the right to be secure against unreasonable search or seizure.

Personal Information Protection and Electronic Documents Act

S.C. 2000, c. 5

Definitions

2 (1) The definitions in this subsection apply in this Part.

[…]

personal information means information about an identifiable individual. (*renseignement personnel*)

[…]

Purpose

3 The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

[…]

Application

4 (1) This Part applies to every organization in respect of personal information that

> **(a)** the organization collects, uses or discloses in the course of commercial activities; or

[…]

Compliance with obligations

5. (1) Subject to sections 6 to 9, every organization shall comply with the obligations set out in Schedule 1.

[…]

7.

[…]

Disclosure without knowledge or consent

(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

> […]
>
> **(c.1)** made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that
>
> > (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
> >
> > (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law,

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or

(iv) the disclosure is requested for the purpose of communicating with the next of kin or authorized representative of an injured, ill or deceased individual;

[…]

When access prohibited

9 (1) Despite clause 4.9 of Schedule 1, an organization shall not give an individual access to personal information if doing so would likely reveal personal information about a third party. However, if the information about the third party is severable from the record containing the information about the individual, the organization shall sever the information about the third party before giving the individual access.

Limit

(2) Subsection (1) does not apply if the third party consents to the access or the individual needs the information because an individual's life, health or security is threatened.

Information related to paragraphs 7(3)**(c), (c.1) or (d)**

(2.1) An organization shall comply with subsection (2.2) if an individual requests that the organization

(a) inform the individual about

(i) any disclosure of information to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d), or

(ii) the existence of any information that the organization has relating to a disclosure referred to in subparagraph (i), to a subpoena, warrant or order referred to in paragraph 7(3)(c) or to a request made by a government institution or a part of a government institution under subparagraph 7(3)(c.1)(i) or (ii); or

(b) give the individual access to the information referred to in subparagraph (a)(ii).

Notification and response

(2.2) An organization to which subsection (2.1) applies

(a) shall, in writing and without delay, notify the institution or part concerned of the request made by the individual; and

(b) shall not respond to the request before the earlier of

(i) the day on which it is notified under subsection (2.3), and

(ii) thirty days after the day on which the institution or part was notified.

Objection

(2.3) Within thirty days after the day on which it is notified under subsection (2.2), the institution or part shall notify the organization whether or not the institution or part objects to the organization complying with the request. The institution or part may object only if the institution or part is of the opinion that compliance with the request could reasonably be expected to be injurious to

(a) national security, the defence of Canada or the conduct of international affairs;

(a.1) the detection, prevention or deterrence of money laundering or the financing of terrorist activities; or

(b) the enforcement of any law of Canada, a province or a foreign jurisdiction, an investigation relating to the enforcement of any such law or the gathering of intelligence for the purpose of enforcing any such law.

Prohibition

(2.4) Despite clause 4.9 of Schedule 1, if an organization is notified under subsection (2.3) that the institution or part objects to the organization complying with the request, the organization

(a) shall refuse the request to the extent that it relates to paragraph (2.1)(a) or to information referred to in subparagraph (2.1)(a)(ii);

(b) shall notify the Commissioner, in writing and without delay, of the refusal; and

(c) shall not disclose to the individual

(i) any information that the organization has relating to a disclosure to a government institution or a part of a government institution under paragraph 7(3)(c), subparagraph 7(3)(c.1)(i) or (ii) or paragraph 7(3)(c.2) or (d) or to a request made by a government institution under either of those subparagraphs,

(ii) that the organization notified an institution or part under paragraph (2.2)(a) or the Commissioner under paragraph (b), or

(iii) that the institution or part objects.

[…]

DIVISION 2

Remedies

Filing of Complaints

Contravention

11 (1) An individual may file with the Commissioner a written complaint against an organization for contravening a provision of Division 1 or 1.1 or for not following a recommendation set out in Schedule 1.

Commissioner may initiate complaint

(2) If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Part, the Commissioner may initiate a complaint in respect of the matter.

Time limit

(3) A complaint that results from the refusal to grant a request under section 8 must be filed within six months, or any longer period that the Commissioner allows, after the refusal or after the expiry of the time limit for responding to the request, as the case may be.

Notice

(4) The Commissioner shall give notice of a complaint to the organization against which the complaint was made.

Investigations of Complaints

Examination of complaint by Commissioner

12 (1) The Commissioner shall conduct an investigation in respect of a complaint, unless the Commissioner is of the opinion that

> **(a)** the complainant ought first to exhaust grievance or review procedures otherwise reasonably available;
>
> **(b)** the complaint could more appropriately be dealt with, initially or completely, by means of a procedure provided for under the laws of Canada, other than this Part, or the laws of a province; or
>
> **(c)** the complaint was not filed within a reasonable period after the day on which the subject matter of the complaint arose.

Exception

(2) Despite subsection (1), the Commissioner is not required to conduct an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a contravention of any of sections 6 to 9 of *An Act to*

promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act.

Notification

(3) The Commissioner shall notify the complainant and the organization that the Commissioner will not investigate the complaint or any act alleged in the complaint and give reasons.

Compelling reasons

(4) The Commissioner may reconsider a decision not to investigate under subsection (1), if the Commissioner is satisfied that the complainant has established that there are compelling reasons to investigate.

Powers of Commissioner

12.1 (1) In the conduct of an investigation of a complaint, the Commissioner may

(a) summon and enforce the appearance of persons before the Commissioner and compel them to give oral or written evidence on oath and to produce any records and things that the Commissioner considers necessary to investigate the complaint, in the same manner and to the same extent as a superior court of record;

(b) administer oaths;

(c) receive and accept any evidence and other information, whether on oath, by affidavit or otherwise, that the Commissioner sees fit, whether or not it is or would be admissible in a court of law;

(d) at any reasonable time, enter any premises, other than a dwelling-house, occupied by an organization on satisfying any security requirements of the organization relating to the premises;

(e) converse in private with any person in any premises entered under paragraph (d) and otherwise carry out in those premises any inquiries that the Commissioner sees fit; and

(f) examine or obtain copies of or extracts from records found in any premises entered under paragraph (d) that contain any matter relevant to the investigation.

Dispute resolution mechanisms

(2) The Commissioner may attempt to resolve complaints by means of dispute resolution mechanisms such as mediation and conciliation.

Delegation

(3) The Commissioner may delegate any of the powers set out in subsection (1) or (2).

Return of records

(4) The Commissioner or the delegate shall return to a person or an organization any record or thing that they produced under this section within 10 days after they make a request to the Commissioner or the delegate, but nothing precludes the Commissioner or the delegate from again requiring that the record or thing be produced.

Certificate of delegation

(5) Any person to whom powers set out in subsection (1) are delegated shall be given a certificate of the delegation and the delegate shall produce the certificate, on request, to the person in charge of any premises to be entered under paragraph (1)(d).

Discontinuance of Investigation

Reasons

12.2 (1) The Commissioner may discontinue the investigation of a complaint if the Commissioner is of the opinion that

(a) there is insufficient evidence to pursue the investigation;

(b) the complaint is trivial, frivolous or vexatious or is made in bad faith;

(c) the organization has provided a fair and reasonable response to the complaint;

(c.1) the matter is the object of a compliance agreement entered into under subsection 17.1(1);

(d) the matter is already the object of an ongoing investigation under this Part;

(e) the matter has already been the subject of a report by the Commissioner;

(f) any of the circumstances mentioned in paragraph 12(1)(a), (b) or (c) apply; or

(g) the matter is being or has already been addressed under a procedure referred to in paragraph 12(1)(a) or (b).

Other reason

(2) The Commissioner may discontinue an investigation in respect of an act alleged in a complaint if the Commissioner is of the opinion that the act, if proved, would constitute a

contravention of any of sections 6 to 9 of *An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act* or section 52.01 of the *Competition Act* or would constitute conduct that is reviewable under section 74.011 of that Act.

Notification

(3) The Commissioner shall notify the complainant and the organization that the investigation has been discontinued and give reasons.

Commissioner's Report

Contents

13 (1) The Commissioner shall, within one year after the day on which a complaint is filed or is initiated by the Commissioner, prepare a report that contains

(a) the Commissioner's findings and recommendations;

(b) any settlement that was reached by the parties;

(c) if appropriate, a request that the organization give the Commissioner, within a specified time, notice of any action taken or proposed to be taken to implement the recommendations contained in the report or reasons why no such action has been or is proposed to be taken; and

(d) the recourse, if any, that is available under section 14.

(2) [Repealed, 2010, c. 23, s. 84]

Report to parties

(3) The report shall be sent to the complainant and the organization without delay.

Hearing by Court

Application

14 (1) A complainant may, after receiving the Commissioner's report or being notified under subsection 12.2(3) that the investigation of the complaint has been discontinued, apply to the Court for a hearing in respect of any matter in respect of which the complaint was made, or that is referred to in the Commissioner's report, and that is referred to in clause 4.1.3, 4.2, 4.3.3, 4.4, 4.6, 4.7 or 4.8 of Schedule 1, in clause 4.3, 4.5 or 4.9 of that Schedule as modified or clarified by Division 1 or 1.1, in subsection 5(3) or 8(6) or (7), in section 10 or in Division 1.1.

Time for application

(2) A complainant shall make an application within one year after the report or notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.

For greater certainty

(3) For greater certainty, subsections (1) and (2) apply in the same manner to complaints referred to in subsection 11(2) as to complaints referred to in subsection 11(1).

Commissioner may apply or appear

15 The Commissioner may, in respect of a complaint that the Commissioner did not initiate,

> **(a)** apply to the Court, within the time limited by section 14, for a hearing in respect of any matter described in that section, if the Commissioner has the consent of the complainant;
>
> **(b)** appear before the Court on behalf of any complainant who has applied for a hearing under section 14; or
>
> **(c)** with leave of the Court, appear as a party to any hearing applied for under section 14.

Remedies

16 The Court may, in addition to any other remedies it may give,

> **(a)** order an organization to correct its practices in order to comply with Divisions 1 and 1.1;
>
> **(b)** order an organization to publish a notice of any action taken or proposed to be taken to correct its practices, whether or not ordered to correct them under paragraph (a); and
>
> **(c)** award damages to the complainant, including damages for any humiliation that the complainant has suffered.

Summary hearings

17 (1) An application made under section 14 or 15 shall be heard and determined without delay and in a summary way unless the Court considers it inappropriate to do so.

Precautions

(2) In any proceedings arising from an application made under section 14 or 15, the Court shall take every reasonable precaution, including, when appropriate, receiving

representations ex parte and conducting hearings in camera, to avoid the disclosure by the Court or any person of any information or other material that the organization would be authorized to refuse to disclose if it were requested under clause 4.9 of Schedule 1.

Compliance Agreements

Compliance agreement

17.1 (1) If the Commissioner believes on reasonable grounds that an organization has committed, is about to commit or is likely to commit an act or omission that could constitute a contravention of a provision of Division 1 or 1.1 or a failure to follow a recommendation set out in Schedule 1, the Commissioner may enter into a compliance agreement, aimed at ensuring compliance with this Part, with that organization.

Terms

(2) A compliance agreement may contain any terms that the Commissioner considers necessary to ensure compliance with this Part.

Effect of compliance agreement — no application

(3) When a compliance agreement is entered into, the Commissioner, in respect of any matter covered under the agreement,

> **(a)** shall not apply to the Court for a hearing under subsection 14(1) or paragraph 15(a); and
>
> **(b)** shall apply to the court for the suspension of any pending applications that were made by the Commissioner under those provisions.

For greater certainty

(4) For greater certainty, a compliance agreement does not preclude

> **(a)** an individual from applying for a hearing under section 14; or
>
> **(b)** the prosecution of an offence under the Act.

Agreement complied with

17.2 (1) If the Commissioner is of the opinion that a compliance agreement has been complied with, the Commissioner shall provide written notice to that effect to the organization and withdraw any applications that were made under subsection 14(1) or paragraph 15(a) in respect of any matter covered under the agreement.

Agreement not complied with

(2) If the Commissioner is of the opinion that an organization is not complying with the terms of a compliance agreement, the Commissioner shall notify the organization and may apply to the Court for

> **(a)** an order requiring the organization to comply with the terms of the agreement, in addition to any other remedies it may give; or
>
> **(b)** a hearing under subsection 14(1) or paragraph 15(a) or to reinstate proceedings that have been suspended as a result of an application made under paragraph 17.1(3)(b).

Time for application

(3) Despite subsection 14(2), the application shall be made within one year after notification is sent or within any longer period that the Court may, either before or after the expiry of that year, allow.

[…]

SCHEDULE 1

4.3 Principle 3 - Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

Note: In certain circumstances personal information can be collected, used, or disclosed without the knowledge and consent of the individual. For example, legal, medical, or security reasons may make it impossible or impractical to seek consent. When information is being collected for the detection and prevention of fraud or for law enforcement, seeking the consent of the individual might defeat the purpose of collecting the information. Seeking consent may be impossible or inappropriate when the individual is a minor, seriously ill, or mentally incapacitated. In addition, organizations that do not have a direct relationship with the individual may not always be able to seek consent. For example, seeking consent may be impractical for a charity or a direct-marketing firm that wishes to acquire a mailing list from another organization. In such cases, the organization providing the list would be expected to obtain consent before disclosing personal information.

4.3.1

Consent is required for the collection of personal information and the subsequent use or disclosure of this information. Typically, an organization will seek consent for the use or disclosure of the information at the time of collection. In certain circumstances, consent with respect to use or disclosure may be sought after the information has been collected but before use (for example, when an organization wants to use information for a purpose not previously identified).

4.3.2

The principle requires “knowledge and consent”. Organizations shall make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used. To make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed.

4.3.3

An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

4.3.4

The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. For example, the names and addresses of subscribers to a newsmagazine would generally not be considered sensitive information. However, the names and addresses of subscribers to some special-interest magazines might be considered sensitive.

4.3.5

In obtaining consent, the reasonable expectations of the individual are also relevant. For example, an individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual’s name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual’s request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

4.3.6

The way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive. Implied consent would generally be appropriate when the information is less sensitive. Consent can also be given by an authorized representative (such as a legal guardian or a person having power of attorney).

4.3.7

Individuals can give consent in many ways. For example:

(a) an application form may be used to seek consent, collect information, and inform the individual of the use that will be made of the information. By completing and signing the form, the individual is giving consent to the collection and the specified uses;

(b) a checkoff box may be used to allow individuals to request that their names and addresses not be given to other organizations. Individuals who do not check the box are assumed to consent to the transfer of this information to third parties;

(c) consent may be given orally when information is collected over the telephone; or

(d) consent may be given at the time that individuals use a product or service.

4.3.8

An individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. The organization shall inform the individual of the implications of such withdrawal.

[…]

4.9 Principle 9 — Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Note: In certain situations, an organization may not be able to provide access to all the personal information it holds about an individual. Exceptions to the access requirement should be limited and specific. The reasons for denying access should be provided to the individual upon request. Exceptions may include information that is prohibitively costly to provide, information that contains references to other individuals, information that cannot be disclosed for legal, security, or commercial proprietary reasons, and information that is subject to solicitor-client or litigation privilege.

4.9.1

Upon request, an organization shall inform an individual whether or not the organization holds personal information about the individual. Organizations are encouraged to indicate the source of this information. The organization shall allow the individual access to this information. However, the organization may choose to make sensitive medical information available through a medical practitioner. In addition, the organization shall provide an account of the use that has been made or is being made of this information and an account of the third parties to which it has been disclosed.

4.9.2

An individual may be required to provide sufficient information to permit an organization to provide an account of the existence, use, and disclosure of personal information. The information provided shall only be used for this purpose.

4.9.3

In providing an account of third parties to which it has disclosed personal information about an individual, an organization should attempt to be as specific as possible. When it is not possible to provide a list of the organizations to which it has actually disclosed information about an individual, the organization shall provide a list of organizations to which it may have disclosed information about the individual.

4.9.4

An organization shall respond to an individual's request within a reasonable time and at minimal or no cost to the individual. The requested information shall be provided or made available in a form that is generally understandable. For example, if the organization uses abbreviations or codes to record information, an explanation shall be provided.

4.9.5

When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending upon the nature of the information challenged, amendment involves the correction, deletion, or addition of information. Where appropriate, the amended information shall be transmitted to third parties having access to the information in question.

4.9.6

When a challenge is not resolved to the satisfaction of the individual, the substance of the unresolved challenge shall be recorded by the organization. When appropriate, the existence of the unresolved challenge shall be transmitted to third parties having access to the information in question.

Canadian Security Intelligence Service Act

R.S.C. 1985, c. C-23

Threats to the Security of Canada

Collection, analysis and retention

12 (1) 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.

No territorial limit

(2) For greater certainty, the Service may perform its duties and functions under subsection (1) within or outside Canada.

Measures to reduce threats to the security of Canada

12.1 (1) If there are reasonable grounds to believe that a particular activity constitutes a threat to the security of Canada, the Service may take measures, within or outside Canada, to reduce the threat.

Limits

(2) The measures shall be reasonable and proportional in the circumstances, having regard to the nature of the threat, the nature of the measures, the reasonable availability of other means to reduce the threat and the reasonably foreseeable effects on third parties, including on their right to privacy.

Alternatives

(3) Before taking measures under subsection (1), the Service shall consult, as appropriate, with other federal departments or agencies as to whether they are in a position to reduce the threat.

Court File No. CV-14-504139

CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION and CHRISTOPHER PARSONS Applicants	-and-	**HER MAJESTY THE QUEEN IN RIGHT OF CANADA, as represented by THE ATTORNEY GENERAL OF CANADA** Respondent

ONTARIO
SUPERIOR COURT OF JUSTICE

PROCEEDING COMMENCED AT
TORONTO

FACTUM OF THE APPLICANTS (RESPONDENTS TO MOTION TO STRIKE), CANADIAN CIVIL LIBERTIES ASSOCIATION AND CHRISTOPHER PARSONS

Paliare Roland Rosenberg Rothstein LLP
155 Wellington Street West
35th Floor
Toronto, ON M5V 3H1

Andrew Lokan (LSUC #31629Q)
Tel.: 416.646.4324
Fax: 416.646.4301
email: andrew.lokan@paliareroland.com

Kartiga Thavaraj (LSO #75291D)
Tel.: 416.646.6317
email: kartiga.thavaraj@paliareroland.com

Lawyers for the Applicants

Doc 2150653 v1