**CITATION:** Canadian Civil Liberties Association v. Canada, 2016 ONSC 4172
**COURT FILE NO.:** CV-14-504139
**DATE:** 20160623

**ONTARIO**

**SUPERIOR COURT OF JUSTICE**

| | | |
|---|---|---|
| **BETWEEN:** | ) | |
| | ) | |
| | ) | |
| CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION AND CHRISTOPHER PARSONS | ) | *Andrew Lokan and Jesse Elders*, for the CCLA and Parsons, Applicants/Responding Parties |
| | ) | |
| Applicants (Respondents to the Motion) | ) | |
| | ) | |
| **– and –** | ) | |
| | ) | |
| HER MAJESTY THE QUEEN IN RIGHT OF CANADA AS REPRESENTED BY THE ATTORNEY GENERAL OF CANADA | ) | *Sean Gaudet and Laura Teskey*, for the Attorney General of Canada. Respondent/Moving Party |
| | ) | |
| Respondent (Moving Party) | ) | |
| | ) | |
| | ) | |
| | ) | **HEARD:** April 14, 2016 |

**R.F. GOLDSTEIN J.**

[1] In a famous dissent the great U.S. Supreme Court Justice Louis Brandeis wrote:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping. Ways may someday be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

[2] Justice Brandeis wrote those prophetic words in 1927: *Olmstead v. United States*, 227 U.S. 438 at p. 475. That case determined that wiretapping in the United States by federal agents was not a violation of the Fourth Amendment, a decision that stood until 1967: *Katz v. United States,* 389 U.S. 347.

[3] We continue to struggle with balancing our right to be secure, as the Fourth Amendment would put it, in our "persons, houses, papers, and effects, against unreasonable searches and seizures" from an astonishing technological capacity.

[4] That astonishing technological capacity exists in the private sector, as more and more of our private life moves into the electronic sphere. The *Personal Information Protection and Electronic Documents Act* is an attempt to regulate and balance the many competing rights and duties of individuals and private businesses. It is federal legislation that regulates the collection, use, and dissemination of personal information by the private sector. The legislation is commonly referred to as PIPEDA.

[5] The government, of course, may seek information from that vast repository for legitimate purposes – and possibly illegitimate purposes. The Applicants, perhaps channelling Justice Brandeis, challenge those sections of PIPEDA that permit a private sector business organization to collect personal information without a person's knowledge and consent, and then disclose it to a government institution – also without a person's knowledge and consent. They also challenge those sections of PIPEDA that may prevent an individual from learning about disclosure of personal information to a government institution. The Applicants say that these sections breach ss. 7 and 8 of the *Canadian Charter of Rights and Freedoms*. The organizations that the Applicants are most concerned about are telecommunications service providers. The government institutions they say collect personal information in violation of the Charter are law enforcement and security intelligence agencies.

[6] The question before the Court on this motion is whether to nip that challenge in the bud or to let it go ahead.

[7] The Attorney General contends that all of the issues relating to the constitutionality of the disclosure provisions of PIPEDA have been dealt with. The Supreme Court of Canada in *R. v. Spencer,* [2014] 2 S.C.R. 212 renders the Application moot. The Attorney General also argues that the Amended Notice of Application should be struck because it fails to disclose a reasonable cause of action.

[8] Procedurally, the Applicants brought a Notice of Application on May 13, 2014. *Spencer* was released on June 17, 2014. The Applicants then filed an Amended Notice of Application on October 31, 2014. The Amended Notice of Application takes the *Spencer* decision into account.

[9] In my respectful view, *Spencer* does not decide the issue. The issue is not moot. I also find that the Amended Notice of Application does disclose a reasonable cause of action. The constitutionality of the sections of PIPEDA challenged by the Applicants is unresolved. The motion is dismissed. The matter can proceed to a full application.

## BACKGROUND

### *(a) The Applicants*

[10] CCLA is an organization that promotes respect for civil liberties in Canada. According to the amended Notice of Application, CCLA historically "has taken principled positions to fight against abuse of authority and threats to fundamental rights and freedoms." Parsons is a member of the CCLA. He is a post-doctoral fellow at the Munk School of Global Affairs at the University of Toronto.

[11] The Attorney General has not – at least at this stage – challenged the standing of the Applicants to bring this Application.

[12] The amended Notice of Application seeks a declaration that ss. 7(3)(c.1), 9(2.1), 9(2.2), 9(2.3), and 9(2.4) of PIPEDA violate s. 7 and s. 8 of the Charter. It is necessary to examine PIPEDA in some detail.

### *(b) The Scheme of PIPEDA:*

[13] The overall nature and purpose of PIPEDA is found in the preamble:

> An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions...

[14] Part 1 of PIPEDA is titled "Protection of Personal Information in the Private Sector". Section 3 sets out the purpose of Part 1:

> 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.

[15] Subsection 5(3) of PIPEDA limits the collection of personal information by an organization. Specifically:

> An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

[16] An "organization" includes a business. Personal information is simply information about an identifiable individual. As I have noted, the organizations that really concern the Applicants are telecommunications service providers.

[17] Section 7 of PIPEDA governs the collection, use, and disclosure of personal information that is collected without the person's knowledge or consent for purposes that are unrelated to business. What the Applicants are specifically concerned about is personal information that may be used for law enforcement or security intelligence purposes.

[18] Section 7(1) is the collection provision. It permits an organization to collect information about an individual under certain circumstances. Of particular note is s. 7(1)(e), which states:

> For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the knowledge or consent of the individual only if
>
> * * *
>
> (e) the collection is made for the purpose of making a disclosure
>
> (i) under subparagraph (3)(c.1)(i)...

[19] Section 7(3)(c.1) of PIPEDA permits disclosure of personal information to "government institutions" under certain circumstances. The government institution must make a request and identify its "lawful authority to obtain the information" and indicate 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.

[20] Subsections 9(2.1) to 9(2.4) of PIPEDA limit what an individual may – or may not – learn about disclosure requests that are made by government institutions. The scheme of this part of PIPEDA works this way:

- An individual seeks to know whether a government institution has requested personal information about him or her under various sections of PIPEDA, including s. 7(3)(c.1). He or she makes a request for information to the organization.

- If there has been disclosure to a government institution, the organization must notify the government institution "without delay and in writing".

- The government institution has 30 days to respond. The government institution must notify the organization if it objects to the organization complying with the request. The government institution may object on the ground that disclosure "could reasonably be expected to be injurious to" any of the following, as set out in subsection 9(2.3):

  > (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.

- The organization must not respond to the request before the earlier of either 30 days from the date it informed the government institution of the request or the date it received a notice that the government institution objects to the request.

***(c) The Alleged Charter Breaches***

[21] The Applicants argue that the disclosure regime governed by PIPEDA violates s. 7 of the Charter because the scope of permissible disclosure of personal information included in s. 7(3)(c.1) is "arbitrary, overbroad and grossly disproportionate. The barriers to obtaining information about whether disclosure has been made further the violation." The Applicants further argue that s. 7(3)(c.1) of PIPEDA violates s. 8 of the Charter. It does so because it "violates the right to be free from unreasonable search and seizure by allowing government access to personal information in a wide range of circumstances absent prior judicial authorization and where individuals hold a reasonable expectation of privacy." The Applicants say that the sections of PIPEDA at issue cannot be saved under s. 1 of the Charter.

[22] The Applicants also challenge ss. 9(2.1), 9(2.2), 9(2.3), and 9(2.4) of PIPEDA. As I have already mentioned, these are the sections that limit the circumstances under which a person may obtain information about a request for information from a government institution. The Applicants have not fleshed out this part of the Application in detail in either the Notice of Application or their factum on this motion.

**ISSUES**

[23] The Attorney General raises two issues:

(a) Is the Application moot?

(b) Does the Amended Notice of Application disclose a reasonable cause of action?

## ANALYSIS

### *(a) Is the Application Moot?*

[24] The Attorney General argues that *Spencer* decides the issue on this Application. Since it is now clear that PIPEDA does not actually authorize a search, there is nothing to challenge. Any government institution conducting a search for personal information covered by s. 7(3)(c.1) requires a source of authority that is not found within PIPEDA. Any search that did not rely on such a source would be a violation of s. 8 of the Charter, as with *Spencer*. Since privacy interests are best viewed through the lens of s. 8, there is no residual basis found in s. 7 of the Charter upon which to challenge PIPEDA. Furthermore, the effect of *Spencer* is not limited to the law enforcement context. It applies equally to intelligence gathering.

[25] I respectfully disagree with the Attorney General. *Spencer* decided a narrow issue within the context of a criminal prosecution. The Applicant's challenge to s. 7(3)(c.1) is much broader. It is a systemic challenge to the scheme for disclosure to government institutions. In particular, *Spencer* did not deal with either intelligence gathering or accountability mechanisms.

*Mootness*

[26] An issue is moot if it is merely hypothetical or abstract: *Borowski v. Attorney General of Canada*, [1989] 1 S.C.R. 342. In *Borowski*, the Supreme Court set out a two-part test for determining whether an issue is moot. The first step is to determine whether the tangible and concrete dispute has disappeared and the issues have become academic. If the answer is "yes", then a court may still elect to hear a case if the circumstances warrant.

*The Decision In Spencer*

[27] In *Spencer*, the Saskatoon Police were searching for anyone who might be sharing child pornography. An officer was able to determine that at least one user in the Saskatoon area was sharing child pornography using LimeWire. LimeWire is file-sharing software that allows others to download content that is stored in a folder on one's computer. LimeWire allows another user to determine the Internet protocol address of a particular computer. It is frequently used to share child pornography. The officer was able to narrow down the geographic location of the computer and determine the telecommunications service provider – in this case Shaw. Based on that information, the officer made a written "law enforcement request" to Shaw for the subscriber information associated to that computer. The officer relied on s. 7(3)(c.1)(ii) of PIPEDA in the "law enforcement request".

[28] Shaw then provided name, address, and telephone number of the subscriber associated with the IP address. It turned out to be Spencer's sister. Spencer lived at his sister's home. The police obtained and executed a search warrant for the address. They seized Spencer's computer. When they analyzed it they found child pornography in his shared LimeWire folder.

[29] Spencer was charged with possession of child pornography and making child pornography available over the internet. His counsel applied to exclude the evidence. He argued that the police request for the subscriber information was a search. Spencer had a reasonable

expectation of privacy in that information. Since there was no judicial authorization, the search was unreasonable and therefore in violation of s. 8 of the Charter. The trial judge disagreed and found that asking for the subscriber information did not constitute a search. The Saskatchewan Court of Appeal agreed. Spencer was convicted.

[30] In the Supreme Court of Canada, Cromwell J., for the unanimous Court, first turned to the question of whether the request constituted a search. Quite simply, if Spencer had a reasonable expectation of privacy in the subscriber information, then the "law enforcement request" constituted a search. Cromwell J. found that it was. After a lengthy analysis, Cromwell J. determined that individuals did indeed have a reasonable expectation of privacy in Internet subscriber information. In coming to that conclusion, Cromwell J. had analyzed the nature of subscriber information. He referred in detail to the provisions of PIPEDA, particularly s. 7 – which he ultimately concluded did not help all that much in determining whether a reasonable expectation of privacy existed in subscriber information. He also analyzed whether subscriber information was part of the core of biographical information that a person would want to keep private from the state – the standard reference for determining the existence of a reasonable expectation of privacy: *R. v. Plant*, [1993] 3 S.C.R. 281 at para. 20. Ultimately, he concluded that it was. The "law enforcement request" was, therefore, a search.

[31] Cromwell J. then analyzed whether the search was lawful. A search is reasonable (and therefore will pass constitutional muster) if it is authorized by law, the law itself is reasonable, and it is carried out in a reasonable manner. The only component of reasonableness at issue in *Spencer* was whether the search was authorized by law.

[32] The Crown had successfully argued at trial and in the Court of Appeal that the combined effect of s. 487.014(1) of the *Criminal Code* and s. 7(3)(c.1)(ii) of PIPEDA granted lawful authority to search.

[33] Cromwell J. disagreed. He found that the combination of the *Criminal Code* and PIPEDA provisions did not authorize a search. His conclusion was based on an analysis of the wording of the two statutes.

[34] Subsection 487.014(1) of the *Criminal Code* at the time of the search stated that:

> For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

[35] That provision is now found in s. 487.0195(1), which is worded slightly differently from the predecessor provision. The provision also takes account of new investigative tools, such as preservation orders:

> For greater certainty, no preservation demand, preservation order or production order is necessary for a peace officer or public officer to ask a person to voluntarily preserve data that the person is not prohibited by law from preserving

> or to voluntarily provide a document to the officer that the person is not prohibited by law from disclosing.

[36] Based on his readings of the two sections, Cromwell J. determined that neither Subsection 487.014(1) of the *Criminal Code* nor s. 7(3)(c.1) of PIPEDA created a search power. The *Criminal Code* provision was simply a declaratory provision that confirmed the existing common law power of the police to make inquiries. It could not be read as going further. As Cromwell J. put it at para. 70:

> On the Crown's reading of these provisions, *PIPEDA*'s protections become virtually meaningless in the face of a police request for personal information: the "lawful authority" is a simple request without power to compel and, because there was a simple request, the institution is no longer prohibited by law from disclosing the information.

[37] Thus, based simply on an analysis of the wording of the legislation, PIPEDA and s. 487.014 did not create a search power.

*Accountability Mechanisms*

[38] A close reading of *Spencer* shows that it decided an important but narrow issue: whether PIPEDA (at least in part) authorized a search in the law enforcement context. The context is important because oversight is automatic in criminal cases where charges are laid. The disclosure process will undoubtedly make the accused person aware of the fact that his or her private electronic information has been accessed by law enforcement. He or she can challenge that in court.

[39] But what of private information that is obtained by law enforcement but no charges are laid? Or inquiries from intelligence agencies that are, by their nature, not intended to be revealed to the person under investigation? In *R. v. Tse*, [2012] 1 S.C.R. 531, the Court considered whether the emergency wiretap provisions in s. 184.4 of the *Criminal Code* were constitutional. Moldaver and Karakatsanis JJ., writing for a unanimous Court, found that they were not. The provision violated s. 8 of the Charter and could not be saved by s. 1. The Court had little difficulty finding that exigent circumstances could justify warrantless wiretapping. Moldaver and Karakatsanis JJ., however, noted that s. 184.4 contained no accountability mechanisms. Unlike the other wiretap provisions, there was no requirement that the target be notified that his or her communications had been intercepted. Moldaver and Karakatsanis JJ. further noted that s. 184.4 had no mechanism for reporting to Parliament – which was also different from other wiretap provisions. Without accountability mechanisms, the provision was unconstitutional. See also: *Wakeling v United States of America*, [2014] 3 S.C.R. 549.

[40] Like s. 184.4 of the *Criminal Code*, PIPEDA contains no accountability mechanisms. There is no mandatory reporting to Parliament, and there is no provision for notifying individuals that their personal information has been the subject of a search. In fact, PIPEDA contains a mechanism to block notification.

[41] This does not mean that s. 7(3)(c.1) of PIPEDA is unconstitutional. Other search and seizure provisions (for example, a report to a justice under Form 5.2 of the *Criminal Code*) may suffice in the law enforcement context. There are certainly some accountability mechanisms built into the *Canadian Security Intelligence Service Act*, but their adequacy and scope was in no way before the Court in *Spencer*. It is also not clear what accountability mechanisms exist for the Communications Security Establishment in the PIPEDA context, either by way of notice to a person whose information has been seized or to Parliament in the form of a reporting requirement. It is, however, clear from *Tse* that the lack of accountability mechanisms may render a regime of search and seizure unconstitutional (even acknowledging that PIPEDA does not create a search power). It is interesting to note that the government has recently introduced legislation that would create a National Security and Intelligence Committee of Parliamentarians. This Committee would, broadly speaking, oversee the national security and intelligence community. The bill had its first Reading on June 16, 2016: Bill C-22, *National Security and Intelligence Committee of Parliamentarians Act.*

*Section 7 of the Charter*

[42] It is unnecessary to delve deeply into the s. 7 aspects of the *Spencer* decision because s. 7 simply was not before the Court. Although I agree with counsel for the Attorney General that an analysis of search and seizure and expectations of privacy is best viewed through the lens of s. 8, that applies in the case of an individual challenge to a particular search: *R. v. Rodgers*, [2006] 1 S.C.R 554 at para. 23. It is less clear whether that principle applies in a broad constitutional challenge.

[43] *Rodgers* did not purport to lay down an inflexible rule. As well, there is certainly authority for the proposition that some highly intrusive searches do engage s. 7 of the *Charter*. In *R. v. Stillman*, [1997] 1 S.C.R. 607, the accused was arrested for murder and detained by police. The police took samples of his hair, saliva, mucous, and pubic hair. A dentist was called in to make dental impressions. These things were all done without the consent of the accused and without judicial authorization. At the time there was no warrant provision in the *Criminal Code* authorizing the taking of bodily samples. The Crown argued that the samples were taken incidental to arrest, a proposition rejected by the majority of the Supreme Court of Canada.

[44] Cory J., for the majority, found that the seizure of the bodily samples was a violation of s. 7 of the Charter (at para. 51):

> The taking of the dental impressions, hair samples and buccal swabs from the accused also contravened the appellant's s. 7 *Charter* right to security of the person. The taking of the bodily samples was highly intrusive. It violated the sanctity of the body which is essential to the maintenance of human dignity. It was the ultimate invasion of the appellant's privacy. See *Pohoretsky, supra*. In *Dyment, supra*, at pp. 431-32, La Forest J. emphasized that "the use of a person's body without his consent to obtain information about him, invades an area of personal privacy essential to the maintenance of his human dignity". Quite simply, the taking of the samples without authorization violated the appellant's

> right to security of his person and contravened the principles of fundamental justice.

[45] I appreciate that the physical security of the person at issue in *Stillman* is different from the informational security of the person at issue in this case. My point is that *Spencer* simply did not deal with s. 7 and that broad constitutional challenges to search and seizure provisions can fall within the ambit of s. 7.

*Conclusion Regarding Mootness*

[46] To summarize:

- The *Tse* issue – accountability – was not before the Court in *Spencer*;
- *Spencer* did not analyze or discuss – or even mention – PIPEDA in the security intelligence context;
- *Spencer* did not deal with requests for information by an individual under ss. 9(2.1) to 9(2.4) of PIPEDA, something that is intimately bound up with the constitutionality of s. 7(3)(c.1); and,
- *Spencer* did not consider the constitutionality of s. 7(3)(c.1) and ss. 9(2.1) to 9(2.4) of PIPEDA with reference to s. 7 of the *Charter*.

[47] The Application is not moot. The Application ultimately may not succeed, but that is not the same thing. I do not need to consider the second part of the *Borowski* test.

***(b) Does the Amended Notice of Application Disclose A Reasonable Cause Of Action?***

[48] Counsel for the Attorney General argues that the Amended Notice of Application fails to disclose a reasonable cause of action because it cannot establish a breach of s. 7 or s. 8. The Application challenges unspecified activities by government institutions made pursuant to sources of authority that are unidentified. The basic flaw in the Amended Notice of Application, according to the Attorney General, is that it fails to take account of the fact that s. 7(3)(c.1) is simply not an authorizing provision. Furthermore, s. 8 of the *Charter* requires that the place to be searched must be the subject of a reasonable expectation of privacy. The references to personal information in the Amended Notice of Application are much too broad. Counsel argues that the existence of a reasonable expectation of privacy in a particular context is fact-specific: *R. v. TELUS Communications Co.*, 2015 ONSC 3964; *R. v. Caza,* 2015 BCCA 374. For that reason, a specific factual context is required to adjudicate on the constitutionality of PIPEDA.

[49] I must respectfully disagree with the Attorney General on this issue as well. I start first with a consideration of Rule 21 and the facts alleged in the Amended Notice of Application.

*Factual Allegations In The Amended Notice of Application*

[50] Under Rule 21, a court must accept the facts in the pleadings as true. A claim should not be struck "if there is a chance that the plaintiff might succeed." It is only where the claim is certain to fail because of a radical defect that the pleading should be struck: *Hunt v. Carey*

*Canada Inc.*, [1990] 2 S.C.R. 959 at para. 36. This applies no less to Notices of Application than it does to Statements of Claim. Where dealing with a Notice of Application, as Brown J. (as he then was) noted in *Barbara Schlifer Commemorative Clinic v. Attorney General of Canada,* 2012 ONSC 5271, "due allowance" must be made for the differences between a notice of application and a statement of claim. A statement of claim requires "a concise statement of the material facts": Rule 25.06(1) of the *Rules of Civil Procedure*. A notice of application requires something different: the precise relief sought, the grounds to be argued, and the documentary evidence to be relied on: see Rule 38.04 of the *Rules of Civil Procedure*. A motion to strike under Rule 21 must be viewed through that lens.

[51] The Applicants rely on the following facts, which must be taken as true for the purposes of a motion to strike:

[52] Parsons, as a post-doctoral fellow, conducts research into privacy issues. His research focuses on how privacy is affected by "digitally mediated surveillance and the implications that such surveillance has in, and on, contemporary Western democracies." Parsons is also concerned with how governments collect and share personal information. As part of his research, Parsons has made requests for information from telecommunications service providers.

[53] Personal information collected by telecommunications service providers is really at the heart of this matter. The Amended Notice of Application states that:

> Government agencies, including the Canada Border Services Agency, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Communications Security Establishment, and provincial and municipal law enforcement authorities seek disclosure of personal information from Canadian telecommunications companies on a massive scale.

[54] In other words, the Amended Notice of Application alleges that law enforcement and security intelligence agencies collect large amounts of personal information. Furthermore,

> A significant majority of these disclosures are made without prior judicial authorization and are rooted in s. 7(3)(c.1) of PIPEDA.

[55] In general, telecommunications providers will not advise individuals if a government institution has requested personal information about them. Some telecommunications service providers will not even disclose the number of requests for personal information made by government institutions.

[56] As I have noted, the Applicants are deeply concerned about disclosure without knowledge and consent to law enforcement and security intelligence agencies. The Canadian Security Intelligence Service and the Communications Security Establishment refuse to disclose the frequency of their requests to telecommunications service providers. Both agencies say that disclosure would harm national security, their ability to collect intelligence, and their ability to advise the government. The RCMP was unable to provide information about the frequency of requests because it does not maintain a central data repository.

[57] The Applicants note that information collected under the PIPEDA regime can be used for both criminal proceedings as well as for intelligence purposes. The information may well be shared with other domestic law enforcement or security intelligence organizations. It may also be shared with foreign law enforcement and intelligence agencies.

[58] The Applicants also note that where personal information is used in a criminal proceeding, the person concerned will learn about it in criminal disclosure. Where it is not used in a criminal proceeding, the fact of disclosure may never be known.

*The Cause of Action*

[59] In my view, the flip side of the lack of mootness is that a cause of action exists at least under s. 8 of the Charter and possibly under s. 7 as well. That has to do not only with the relief sought in this motion, but also with the nature of an application.

[60] There are practical reasons of judicial economy why motions to strike an application should granted sparingly. An application is in many ways like a motion – a summary procedure that relies (for the most part) on affidavit evidence and bare pleadings. The time and resources spent on a motion to strike an application may be equal to the time and resources spent on the application itself. I agree with the observation of Strayer J.A. in the Federal Court of Appeal that the most economical way to deal with an application that is without merit is often to simply argue the application, rather than engage in interlocutory proceedings: *David Bull Laboratories (Canada) Inc. v. Pharmacia Inc.*, [1995] 1 F.C.R. 588 (C.A.).

[61] Furthermore, it is well-established that the motion to strike must be used with care. As McLachlin C.J. noted for the Supreme Court in *R. v. Imperial Tobacco Canada Ltd.*, [2011] 3 S.C.R. 45 at para. 21:

> Valuable as it is, the motion to strike is a tool that must be used with care. The law is not static and unchanging. Actions that yesterday were deemed hopeless may tomorrow succeed. Before *Donoghue v. Stevenson*, [1932] A.C. 562 (H.L.) introduced a general duty of care to one's neighbour premised on foreseeability, few would have predicted that, absent a contractual relationship, a bottling company could be held liable for physical injury and emotional trauma resulting from a snail in a bottle of ginger beer. Before *Hedley Byrne & Co. v. Heller & Partners Ltd.*, [1963] 2 All E.R. 575 (H.L.), a tort action for negligent misstatement would have been regarded as incapable of success. The history of our law reveals that often new developments in the law first surface on motions to strike or similar preliminary motions, like the one at issue in *Donoghue v. Stevenson*. Therefore, on a motion to strike, it is not determinative that the law has not yet recognized the particular claim. The court must rather ask whether, assuming the facts pleaded are true, there is a reasonable prospect that the claim will succeed. The approach must be generous and err on the side of permitting a novel but arguable claim to proceed to trial.

*Section 8 of the Charter*

[62] I agree with the Applicants that s. 8 of the *Charter* is engaged because PIPEDA is part of a regime of seizure of personal information and disclosure to law enforcement or security intelligence agencies. PIPEDA, as I dealt with earlier in these reasons, has no oversight mechanism. An oversight mechanism is critical for constitutionality. Whether oversight mechanisms that may exist in the *Criminal Code* and other legislation are adequate is surely a question that should be fleshed out during the course of a full application.

*Section 7 of the Charter*

[63] With regard to s. 7 of the *Charter*, the Applicants make four points:

- First, the Applicants say that the lack of an oversight and accountability mechanism violates s. 7 as well as s. 8 of the *Charter*. Information seized in the context of the PIPEDA regime, they argue, violates a person's right to informational privacy in a manner that is not in accordance with the principles of fundamental justice.
- Second, the Applicants also argue that the reference to "lawful authority" is impermissibly vague.
- Third, s. 7(3)(c.1) of PIPEDA is legislation that is arbitrary, overbroad, and grossly disproportionate to the ends it seeks to achieve
- Fourth, the Applicants argue that s. 7(3)(c.1) of PIPEDA leaves it to individual organizations and businesses to determine their level of compliance with law enforcement and security intelligence requests for information. This provision, they argue, leaves it to an organization, rather than an independent judicial officer, to determine whether and how to respond.

[64] Counsel for the Attorney General argues that a court should not engage in a discussion of s. 7 of the *Charter* because the constitutionality of searches is best dealt with under the rubric of s. 8: see *R. v. Rodgers*. As a general proposition, that is obviously correct in the context of routine challenges in individual cases. I do not agree, however, that the challenge as framed under s. 7 has no chance of success. This application is a systemic challenge rather than an attack on any particular search.

[65] The Applicants attack s. 7(3)(c.1) of PIPEDA on other bases as well: they argue that the legislation is impermissibly vague. That is obviously an argument under s. 7. The Applicants also argue that PIPEDA currently leaves it to individual telecommunications service providers to determine whether and how a "law enforcement request" should be complied with, even after *Spencer*. That question clearly engages s. 7 of the *Charter* since it is at least debatable whether that delegation of discretion is in accordance with the principles of fundamental justice.

[66] The Applicants further argue that the scope of permissible disclosure of personal information remains arbitrary, overbroad, and grossly disproportionate even after *Spencer*. Spencer did not any any way deal with those three concepts. Those concepts fall under the rubric of s. 7 of the *Charter*. In *Bedford v. Canada*, [2013] 3 S.C.R. 110 Chief Justice

McLachlin, writing for the Court, discussed these concepts in detail at paras. 93-123. Of particular note for the purposes of this motion are paras. 108-109:

> The case law on arbitrariness, overbreadth and gross disproportionality is directed against two different evils. The first evil is the absence of a connection between the infringement of rights and what the law seeks to achieve -- the situation where the law's deprivation of an individual's life, liberty, or security of the person is not connected to the purpose of the law. The first evil is addressed by the norms against arbitrariness and overbreadth, which target the absence of connection between the law's purpose and the s. 7 deprivation.
>
> The second evil lies in depriving a person of life, liberty or security of the person in a manner that is grossly disproportionate to the law's objective. The law's impact on the s. 7 interest is connected to the purpose, but the impact is so severe that it violates our fundamental norms.

[67] It may be that Counsel for the Attorney General is ultimately right that these issues ought to be decided under s. 8 of the Charter, but at this stage I am not prepared to strike the Amended Notice of Application on that basis. It is a novel claim, and novelty is no reason to strike a pleading.

**DISPOSITION**

[68] The matter can proceed to a full application. The motion is dismissed.

**COSTS**

[69] The Applicants, as the successful party, may submit a costs outline and submissions of no more than two pages within 30 days of the release of this judgment. The Respondent may submit a costs outline and submissions of no more than two pages within 30 days of receiving the Applicant's costs outline and submissions.

R.F. Goldstein J.

**Released:** June 23, 2016

**CITATION:** Canadian Civil Liberties Association v. Canada, 2016 ONSC 4172
**COURT FILE NO.:** CV-14-504139
**DATE:** 20160623

**ONTARIO**

**SUPERIOR COURT OF JUSTICE**

**BETWEEN:**

CORPORATION OF THE CANADIAN CIVIL LIBERTIES ASSOCIATION AND CHRISTOPHER PARSONS

Applicants
(Respondents to the Motion)

– and –

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

Respondent
(Moving Party)

---

**REASONS FOR JUDGMENT**

---

R.F. Goldstein J.