Canadian Journal of Law and Technology

Volume 14 | Number 1 Article 6

1-1-2016

Is There a 'Right to be Forgotten' in Canada's Personal Information Protection and Electronic Documents Act (PIPEDA)?

Michael Rosenstock

Is there a 'right to be forgotten' in Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)?*

Michael Rosenstock[*]

INTRODUCTION

In May 2014, the Court of Justice of the European Union (the EU Court) held that internet search engines must remove search results that link to non-defamatory information about an individual that are "no longer necessary in the light of the purposes for which they were collected or processed."[1] The Court stated that this test would likely be met when the information was inaccurate, inadequate, irrelevant, excessive, or out-of-date.[2] Importantly, even though the search results that satisfy this test would be removed, the underlying content would remain on the internet.[3]

Google Spain was widely viewed as formally recognizing an individual's "right to be forgotten" on the internet,[4] and led Google[5] and other search engines[6] to implement processes through which individuals could seek the removal of information from internet searches conducted in Europe. In the eight months following the decision, 175,000 people applied to Google for the removal of 600,000 internet links. The search engine approved about 40% of those requests.[7] Beyond this response, the decision has potentially far-reaching

---

[*] B.A., M.A., J.D. The author is currently a Judicial Law Clerk at the Ontario Superior Court of Justice in Toronto. This article is written in a personal capacity and does not in any way reflect the views of the Ontario Superior Court of Justice or the Ministry of the Attorney General. The author can be contacted at michael.j.rosenstock@gmail.com.

1 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (May 13, 2014), Doc. C-131/12 (European Court of Justice (Grand Chamber)) at para. 93 [*Google Spain*].

2 *Ibid* at paras. 92-93.

3 *Ibid* at para. 62.

4 See e.g. Alan Travis and Charles Arthur, "EU court backs 'right to be forgotten': Google must amend results on request", *The Guardian* (13 May 2014), online: < www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results > .

5 Google Inc., "Search removal request under data protection law in Europe", online: < https://support.google.com/legal/contact/lr_eudpa?product = websearch&hl = en > .

6 See e.g. Bing, "Request to Block Bing Search Results In Europe", online: < https://www.bing.com/webmaster/tools/eu-privacy-request > .

7 Google Inc., "Transparency Report — European Privacy Requests for Search Removals", online: < https://www.google.com/transparencyreport/removals/europe-privacy > .

implications for the ways in which the internet is used to disseminate information.

One view of *Google Spain* is that it reflects law and policy unique to Europe. Indeed, the decision was based largely on an exercise in statutory interpretation of European Directive 95/46/EC, which is aimed at ensuring data processing systems protect privacy rights.[8] Further, the Directive is considered a relatively "robust" application of Fair Information Practices,[9] a common privacy framework developed through the Organization of Economic Cooperation and Development (OECD) and implemented differently throughout the world.[10] Finally, the Directive[11] and the EU Charter[12] establish privacy rights as "fundamental freedoms", which is viewed as a response to Europe's history with communist and fascist regimes that made extensive and malevolent use of personal information.[13]

However, Canada's *Personal Information Protection and Electronic Documents Act* (*PIPEDA*)[14] also establishes a privacy right with respect to personal information based on the Fair Information Practice framework,[15] and imposes similar obligations on organizations that collect, use or disclose personal information. Moreover, Canadian courts have recognized the "quasi-constitutional" status of privacy rights.[16] Thus, while the general consensus appears to be that a right to be forgotten does not exist in Canadian law, some

---

8 See EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281/31 at Art 1 [Directive].

9 Lisa M Austin, "Enough About Me: Why Privacy is About Power, Not Consent (or Harm)" at 136 in Austin Sarat, ed., *A World Without Privacy?* (Cambridge, UK: Cambridge University Press, 2015).

10 OECD, *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (23 September 1980)*, online: <www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#recommendation>; See also Austin (2015), *ibid* at 136.

11 Directive, *supra* note 8 at Preamble (2) and Art 2.

12 EC, *Charter of Fundamental Rights of the European Union*, [2000] OJ, C 364/01 at Art 11 [EU Charter].

13 Jeffrey Toobin, "The Solace of Oblivion", *The New Yorker* (29 Sep 2014), online: <www.newyorker.com> (quoting Viktor Mayer-Schönberger).

14 *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 [*PIPEDA*].

15 Austin (2015), *supra* note 9 at 136.

16 See e.g. *UFCW, Local 401 v. Alberta (Information and Privacy Commissioner)*, 2013 SCC 62, 2013 CarswellAlta 2210, 2013 CarswellAlta 2211, (*sub nom. Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*) [2013] 3 S.C.R. 733, [2013] S.C.J. No. 62 (S.C.C.) at para. 22 [*Alberta Privacy Commissioner*]. See also *Eastmond v. Canadian Pacific Railway*, 2004 FC 852, 2004 CarswellNat 1842, 2004 CarswellNat 3545, [2005] 2 F.C.R. D-32, [2004] F.C.J. No. 1043 (F.C.) at para. 100.

have speculated that there may be a "legitimate case" for a similar result in Canada.[17]

In this paper, I argue that *PIPEDA* could support a version of the right to be forgotten, subject to three important caveats. First, for search engines to meet the threshold applicability test under *PIPEDA*, their activities (i.e., crawling, indexing, organizing, etc.) must constitute the "collection, use or disclosure" of personal information. Ascribing such a role to search engines in information dissemination would likely require a court to distinguish the activities of search engines from hyperlinks on websites, which the Supreme Court in *Crookes v. Newton* determined did not involve control over content.[18] Second, *PIPEDA*'s "all-or-nothing approach"[19] means that if search engines met the threshold test, a series of obligations would be imposed on them regardless of their practicality, suitability or intelligibility. One of these obligations — to which exemptions are limited — would require search engines to obtain (and maintain) consent from individuals to collect, use or disclose their personal information. A court may react to the significant challenges of "fitting" *PIPEDA* to search engines by rejecting the application of *PIPEDA* at the threshold stage. Third, as the breadth of the right to be forgotten articulated in *Google Spain* would likely infringe the "core" of Canadian *Charter* protections for freedom of expression, one would expect any right recognized under *PIPEDA* to be far narrower than that under the Directive.

This paper proceeds as follows: Section 2 describes and contrasts the EU Directive and *PIPEDA*; Section 3 reviews and critically assesses *Google Spain*; Section 4 examines whether a right to be forgotten could be discovered in *PIPEDA*; Section 5 concludes.

I. THE EU DIRECTIVE AND CANADA'S *PIPEDA*

Both the EU Directive and *PIPEDA* establish a right of privacy with respect to the processing of personal information.[20] As noted in the introduction, the Directive (and the EU Charter) characterizes this right as a "fundamental right", whereas *PIPEDA* makes no such express claim. Both legislative frameworks define "personal data" (Directive) or "personal information" (*PIPEDA*) broadly to mean information about an identifiable individual, without regard to whether

---

[17] See Andre Mayer, "'Right to be forgotten': How Canada could adopt similar law for online privacy" *CBC News* (16 June 2014), online: <www.cbc.ca> (Quoting lawyer Kristen Thompson); Justin Ling, "Forget me, Google", *National* (May 2014), online: <www.nationalmagazine.ca>. See also John Wunderlick, "A Limited Empowerment" (June 2014) Privacy Journal 1 at 4.

[18] *Crookes v. Wikimedia Foundation Inc.*, 2011 SCC 47, 2011 CarswellBC 2627, 2011 CarswellBC 2628, (*sub nom. Crookes v. Newton*) [2011] 3 S.C.R. 269, [2011] S.C.J. No. 47 (S.C.C.) at para. 26 (per Abella J) [*Newton*].

[19] Lisa M Austin, "Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices" (2006) 44 Can Bus LJ 21 at 28.

[20] *PIPEDA*, *supra* note 14 at s. 3; Directive, *supra* note 8 at Art 1(1).

the personal information is publicly available.[21] If the activity falls within the scope of the Directive or *PIPEDA*, the legislative frameworks impose a range of obligations. I discuss the threshold question before turning to the substantive obligations. For convenience, Table 1 in the Appendix reproduces and compares the relevant sections of the Directive and *PIPEDA*.

(a) Threshold questions

Arguably where the Directive and *PIPEDA* exhibit the most differences relates to the threshold questions of application and jurisdiction: whether the law applies to the organization and the kinds of activities it engages in (application), and the extent to which the law applies to organizations that operate outside of Canada or Europe (jurisdiction or "territoriality"). The concepts of application and jurisdiction are intertwined as they rely on the same statutory provisions and terminology.

Articles 3 and 4 of the Directive together define the criteria for the Directive to apply and for an EU Member State to assert jurisdiction. Article 3 states that the Directive will apply to "the processing of personal data wholly or partly by automatic means."[22] The processing of personal data is defined broadly as "any operation. . .performed upon personal data", and includes collection, use and disclosure and over ten additional activities (e.g., recording, storage, retrieval, and "making available").[23] Article 4 lists connecting factors that authorize a Member State to assume jurisdiction over the processing of personal data. The most relevant connecting factor to this paper is that jurisdiction can be assumed when the processing of personal data is "carried out in the context of the activities of an establishment of the controller on the territory of the Member State."[24] A controller is defined as the person that "determines the purposes and means of the processing of personal data."[25]

Section 4 of *PIPEDA* provides that the statute applies "to every organization in respect of personal information that . . . the organization collects, uses or discloses in the course of commercial activities."[26] *PIPEDA* thus applies to a narrower set of activities than the Directive: *PIPEDA* imposes a commercial character requirement, and only three of the activities ("collects, uses or discloses") identified by the Directive fall under the scope of *PIPEDA*.[27]

---

[21] Directive, *supra* note 8 at Art 2(a); *PIPEDA*, *supra* note 14 at s. 2 ("personal information"); Office of the Information Commissioner of Canada, "Interpretation Bulletin — Personal Information" (2013), online: <https://www.priv.gc.ca/leg_c/interpretations_02_e.asp>.

[22] Directive, *supra* note 8 at Art 3(1).

[23] *Ibid* at Art 2(b).

[24] *Ibid* at Art 4(1)(a).

[25] *Ibid* at Art 2(d).

[26] *PIPEDA*, *supra* note 14 at s. 4(1)(a).

[27] See *ibid* at 2 ("commercial activity").

PIPEDA does not establish the conditions for the assumption of jurisdiction. "Organization" is defined to include a corporation, but does not require that, for example, the company be incorporated in Canada, or collect, use or disclose personal information within Canadian borders.[28] The issue of jurisdiction is thus left to statutory interpretation in combination with common law principles — specifically the "real and substantial connection" test.[29] The effect of these differences is that *PIPEDA* may have greater extraterritorial reach than the Directive.

The Directive and *PIPEDA* also contain a number of across-the-board exemptions. Most prominently, both legislative frameworks fully exclude the processing of personal data (Directive) or the collection, use or disclosure of personal information (*PIPEDA*) *solely* for journalistic, artistic or literary purposes. Given the significant restrictions imposed on this exemption (i.e., "solely"), the exemptions are not available to search engines,[30] although the exemption is available to the operators of many of the underlying websites listed in search results (e.g., websites of media organizations).[31]

(b) Substantive obligations

If the threshold criteria are met, both the Directive and *PIPEDA* impose a range of obligations, the most significant of which is the requirement that individual consent be obtained before processing personal data or collecting, using or disclosing personal information.[32] While both legislative frameworks provide exemptions to the consent obligation, the exemptions contained in the Directive are broader and more flexible. Article 7(f) of the Directive permits personal data to be processed without consent when it is "necessary for the purposes of the legitimate interests pursued by the controller", unless those legitimate interests are "overridden" by fundamental freedoms (e.g., privacy rights). Rather than subjecting the consent obligation to a balancing test, *PIPEDA* lists several circumstances whereby consent is not required. The most relevant of these circumstances is where the information is publicly available *and* specified by the regulations.[33] *PIPEDA* regulations specify the following classes of information: name and contact information published in telephone and business directories; information from a registry "collected under a statutory authority"; information disclosed in legal proceedings associated with a judicial

---

[28] *Ibid* at s. 2 ("organization").

[29] See *Lawson v. Accusearch Inc.*, 2007 FC 125, 2007 CarswellNat 247, 2007 CarswellNat 853, [2007] 4 F.C.R. 314, [2007] F.C.J. No. 164 (F.C.) at paras. 34, 38-43 [*Lawson*].

[30] There may be an argument for the exclusion of Google News (a news aggregator) under the journalistic exemption, a point that I leave for future research.

[31] See *PIPEDA*, *supra* note 14 at s. 4; Directive, *supra* note 8 at Arts 8-9.

[32] *PIPEDA*, *supra* note 14 at s. 7 and Sch 1 at s. 4.3; Directive, *supra* note 8 at Art 7(f). Article 7 of the Directive establishes other exemptions to the consent obligation beyond the scope of this paper.

[33] *PIPEDA*, *supra* note 14 at ss 7(1)(d), 7(3)(h.1), 7(4), 7(5).

or quasi-judicial body; and personal information that appears in a publication "where the individual has provided the information".[34]

Irrespective of whether the activity is exempted from the consent obligation, both the Directive and *PIPEDA* impose a number of additional obligations that, *inter alia*, limit the processing of personal information and ensure its accuracy. The Directive states that personal data must be "adequate, relevant and not excessive" and "accurate, and where necessary, kept up to date" in relation to the purpose for which the data is collected.[35] *PIPEDA* requires that the collection of personal information is "limited to that which is necessary for the purposes identified by the organization", not collected "indiscriminately", "retained only as long as necessary" and be "accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used."[36] Despite the differences in terminology, a close comparison reveals that the obligations are substantively similar. I refer to these obligations throughout this paper as the "accuracy and use limitation obligations".

The Directive and *PIPEDA* also provide similar remedies to individuals to enforce privacy rights. Under Article 12 of the Directive and Principle 9 of *PIPEDA*, individuals are provided a right to access their personal information held by an organization and the right to challenge the organization on the accuracy and completeness of that information.[37] Inaccurate or incomplete data must be corrected or erased, as appropriate. Where personal data are being processed without an individual's consent (i.e., through the exemption described above), Article 14 of the Directive provides an additional right to individuals to object to the processing on "compelling legitimate grounds."[38] *PIPEDA* does not provide a similar right of objection, but as noted above, the ability of organizations to collect personal data without consent is more constrained.

II. THE *GOOGLE SPAIN* DECISION

(a) Overview

In *Google Spain*, Spanish resident Mario Costeja González filed a complaint with the Spanish Data Protection Agency (AEPD) against Google Spain, Google Inc. and a Spanish newspaper. Fifteen years earlier, the newspaper published an announcement of a real estate auction to recover social security debts he owed, and hyperlinks to the announcement appeared in a Google search of his name.[39]

---

[34] SOR/2001-7 at s. 1. Other exemptions are provided but are not relevant to this analysis. See generally *PIPEDA*, *ibid* at s. 7(1). In addition, *PIPEDA* requires that the purposes for personal information collection, use or disclosure be "appropriate in the circumstances": see *PIPEDA*, *ibid* at s. 5(3).

[35] Directive, *supra* note 8 at Art 6(c) and (d).

[36] *PIPEDA*, *supra* note 14 at Sch 1 at ss 4.4, 4.5 and 4.6.

[37] Directive, *supra* note 8 at Art 12; *PIPEDA*, *supra* at Sch 1 s. 4.9.

[38] Directive, *ibid* at Art 14(a).

The publication was not alleged to be defamatory. Nevertheless, Costeja González sought orders against the newspaper to delete the publication and against Google to remove the publication from search results on the basis that they conflicted with the Directive. The AEPD refused the request with regards to the newspaper, but agreed to the order against Google. The decision was appealed to the EU Court. The EU Court agreed substantially with the AEPD and ruled that the Directive required Google to remove the newspaper publication from search results.

(b) Interpretation of the Directive in Google Spain

In *Google Spain*, the EU Court was tasked with interpreting three aspects of the Directive: application, jurisdiction, and the scope of the obligation on Google.[40] In the following discussion, note that any reference to "Google" refers to Google Inc., the operator of the search engine based in the United States — as opposed to Google Spain, a subsidiary incorporated in Spain to sell online advertising to local firms.[41]

(i) Application

Google argued that the Directive ought not to apply because it was not engaged in the "processing of personal data": the search engine crawled and indexed *all* of the information on the internet without regard to whether the information was "personal data."[42] The EU Court rejected this argument. It determined that at least some of the information "found, indexed and stored" by search engines and listed in search results were personal data in that it related to identified persons, and the definition does not require any differentiation between "personal data" and other data. Further, the search engine's activities met the broad definition of "processing of personal data": crawling webpages constituted "collection"; indexing represented "retrieval", "recording", "organization" and "storage"; and listing the search results comprised "disclosure" and "making available" of personal data.[43] (The EU Court made no finding that Google "used" personal data.)

---

[39] *Google Spain*, *supra* note 1 at para. 14.

[40] *Ibid* at para. 20.

[41] See *ibid* at para. 44.

[42] *Ibid* at para. 22.

[43] *Ibid* at paras. 26-31. Although this was not made explicit in the decision, a search through Google (or any other search engine) does not scour all the webpages of the internet in real time. Rather, Google continuously crawls websites and builds an index of the internet. Google searches are conducted on the index: See Google Inc., "How search works", online: <www.google.ca/insidesearch/howsearchworks/thestory> (Accessed 4 Nov 2014).

(ii) Jurisdiction

Concluding that the search engine engaged in the "processing of personal data" led the EU Court to find that Google was a "controller" within the meaning of the Directive — through the crawling and indexing activities, the search engine determined the "purposes and means" of the data processing.[44] The more difficult issue was whether the processing was "carried out in the context of the activities of an establishment [Google Spain] of the controller [Google]."[45] Google argued that this could not be the case because its activities were legally distinct from Google Spain.[46] The EU Court held that because the Directive employs the phrase "in the context *of* the activities" rather than "*by* the activities", Google Spain did not have to be a data processor to meet the terms of the connecting factor.[47] The fact that Google Spain sold advertising displayed in Google searches — making the search function profitable — was sufficient to establish the necessary context.[48]

(iii) Scope of obligation on Google

In determining the obligation on Google as a processor of personal data, the EU Court rejected two arguments submitted by the search engine. First, Google suggested that requests to erase content ought to be made exclusively to the publisher of the underlying website. The EU Court held that Google was not a passive information intermediary. Rather, it created content by permitting users to obtain a "structured overview" of personal data and a "detailed profile of the data subject" — information that would not be easily attainable without search engines.[49] Requiring the removal of content from individual webpages would insufficiently protect privacy because the information contained in underlying webpages could easily be duplicated, and media were exempted from the Directive.[50] Second, Google argued that ordering it to remove content violated the "fundamental rights" (i.e., freedom of expression) of the search engine and internet users.[51] The EU Court agreed that internet users had a "legitimate interest" in accessing information on the internet, but described the interests served in the processing of personal data as largely economic.[52] Given the importance attached to privacy rights in the Directive and EU Charter[53], as a

---

44 *Google Spain*, *supra* note 1 at paras. 32-34.

45 Directive, *supra* note 8 at Art 4(1)(a).

46 *Google Spain*, *supra* note 1 at para. 51.

47 *Ibid* at para. 52 (emphasis added).

48 *Ibid* at paras. 52, 56.

49 *Ibid* at paras. 37, 80.

50 *Ibid* at para. 84-85.

51 *Ibid* at para. 63.

52 *Ibid* at para. 81.

53 See EU Charter, *supra* note 12 at Art 7 (Respect for private and family life) and Art 8 (Protection of personal data).

"general rule" the privacy rights would prevail over the economic interests of Google.[54]

The EU Court interpreted Articles 12 and 14 as tasking the search engine with evaluating and acting upon requests by EU residents to remove search results, with recourse to domestic data regulators and the courts. Google must remove search results that violate Article 6 of the Directive: that is, when the search results are inaccurate, inadequate, irrelevant, excessive, not up-to-date, or kept longer than necessary.[55] However, where the benefits of making information accessible to the public more than offset the privacy infringement, the balancing test contained in Article 7(f) requires Google to reject the individual's request. The EU Court held that the public would have a greater interest in access to information when that individual played a more significant role in public life.[56] In other words, requests under the right to be forgotten would be subject to a case-by-case assessment.

Applied to the facts of the case, the EU Court held that given the amount of time that had passed since the real estate auction, the "sensitivity" of the information to Costeja González's private life, and the lack of public interest in accessing such information, Google must remove the link to the newspaper publication from the search results.[57]

(c) Analysis

This paper focuses on two related aspects of the *Google Spain* decision: freedom of expression and the requirement that search engines administer requests to delete search results.

(i) Freedom of expression

The most controversial aspect of *Google Spain* and the right to be forgotten more generally relates to freedom of expression. American privacy scholar Jeffrey Rosen labeled the right to be forgotten as the "biggest threat to free speech on the Internet in the coming decade."[58] Other scholars and media, particularly in the US, UK, and Canada, have expressed similar sentiment.[59]

Freedom of expression received surprisingly little attention in *Google Spain*. In fact, while citing the privacy protections contained in the EU Charter, the EU Court did not make a single reference to Article 11, which states:

---

54 *Google Spain*, *supra* note 1 at para. 81.

55 *Ibid* at paras. 79, 81, 94-99.

56 *Ibid* at para. 97.

57 *Ibid* at para. 98.

58 Jeffrey Rosen, "The Right to Be Forgotten" (2012) 64 Stan L Rev Online 88 at 88.

59 See e.g. Michael Geist, "'Right to be forgotten' ruling lacks balance", *Toronto Star* (16 May 2014) B4; Juergen Baetz, "Media outlets cry censorship as Google removes certain search results in Europe", *Globe and Mail* (4 Jul 2014) B7.

> Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to *receive and impart information and ideas* without interference by public authority and regardless of frontiers.[60]

Paradoxically, in reasoning that Google was a "controller" under the Directive, the EU Court held that the search engine "plays a decisive role" in transmitting information[61] — the same factors which ought to have led the EU Court to inquire into the impact of a right to be forgotten on freedom of expression. Requiring a search engine to remove search results suppresses the capacity of website publishers and internet users to "receive and impart information and ideas."[62] Website publishers — including media organizations — whose webpages are de-linked from search engine indexes are constrained from reaching audiences ("impart"). Likewise, internet searches would lead users to incomplete or less relevant information ("receive"). The significance of search engines in communicating information should not be understated: a 2014 poll, for example, found that half of Americans found their news through search engines.[63]

The consequence of ignoring freedom of expression is that privacy rights are protected as a "fundamental freedom", while the interests of publishers and internet users in search results are left unarticulated and hollow. A balancing test that pits a fundamental freedom against something less (e.g., a commercial interest) will almost always favour the fundamental freedom. Describing the interests of website publishers and internet users in search results as a "fundamental freedom" would have significantly reshaped the balancing test, making the outcome far less clear (and far more complex). This is not to say that freedom of expression should necessarily defeat privacy rights, only that they should factor significantly into the balancing exercise.

Beyond the legal analysis is a crucial normative question about the extent to which information posted online should be indefinitely available and accessible. In *Google Spain*, the complainant was unable to shed his bankruptcy troubles

---

60 *EU Charter*, *supra* note 12 at Art 11 (emphasis added).

61 See *Google Spain*, *supra* note 1 at para. 36.

62 Others have argued for greater consideration of the public interest in accessing information through search results. These include the Advocate General who brought the case to the EU Court: Opinion of Advocate General Jääskinen, *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (June 25, 2013), Doc. C-131/12 at paras. 120-125. See also Christopher Rees and Debbie Heywood, "The 'right to be forgotten' or the 'principle that has been remembered'" (2014) 30:5 Computer L & Sec Report 574 at 578; Ann Cavoukian and Christopher Wolf, "The web never forgets (nor should it)", *National Post* (25 Jun 2014) A13; Dominic McGoldrick, "Developments in the Right to be Forgotten" (2013) 13:4 Human Rights Law Review 761 at 766.

63 American Press Institute, "How Americans get their news" (17 Mar 2014), online: < www.americanpressinstitute.org/publications/reports/survey-research/how-americans-get-news > .

from over a decade earlier. There are more compelling examples: a 73-year-old teacher terminated after students learned through the Internet Movie Database (IMBd) that she acted in erotic films in her twenties;[64] a sexual assault victim seeking to remove her name from a news article describing the violence;[65] or a high school student concerned about being denied university admission because of a five-year-old "tweet".[66] Viktor Mayer-Schönberger argues that "digital memory" has led to the end of forgetting, and endorses legal frameworks such as the right to be forgotten as a means of encouraging forgiveness.[67] This essay cannot canvass this discussion in detail, but these issues are critical to understanding the other side of the free speech debate.

(ii) Role of search engine

The decision to task Google with evaluating requests and deleting search results has also been subject to significant criticism. A number of commentators draw an analogy between search engines and libraries,[68] and argue that forcing Google to remove search results is akin to requiring libraries to remove titles from electronic indices — which is antithetical to their purpose of providing users with "materials from which they can make their own judgment."[69] Ultimately this criticism is rooted in a starkly different characterization of the role played by search engines in information dissemination. The EU Court determined that search engines do not simply make information easier to find: they permit users to obtain a "structured overview" of a person that contains a "more or less detailed profile."[70] Anyone that has searched their own name and found their picture, employment history, or educational background on the first page of search results would likely find some merit in this argument. Similar information of the same quality and volume is not accessible from a library.[71] Whether or not

---

64 Graeme Hamilton, "Risqué film corpus used as dismissal grounds", *National Post* (21 Oct 2014) A3.

65 See Google, "Examples of requests we encounter", online: <https://www.google.com/transparencyreport/removals/europeprivacy>.

66 See Natasha Singer, "They Loved Your GPA Then They Saw Your Tweets", *New York Times* (9 Nov 2013), online: <www.nytimes.com>.

67 See Viktor Mayer-Schönberger, "Omission of search results is not a 'right to be forgotten' or the end of Google", *The Guardian* (13 May 2014), online: <www.theguardian.com>; Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton: Princeton University Press, 2012) at 4, 207-209.

68 Cavoukian and Wolf, *supra* note 62 at A13; "On being forgotten", *The Economist* (17 May 2014), online: <www.economist.com>; David Drummond, "We need to talk about the right to be forgotten", *The Guardian* (10 Jul 2014), online: <www.theguardian.com>; Jodie Ginsberg, "Right to be forgotten: A poor ruling, clumsily implemented", *Index on Censorship* (3 Jul 2014), online: <indexoncensorship.org>. *But see* Toobin, *supra* note 13 (quoting privacy advocate Marc Rotenberg).

69 Cavoukian and Wolf, *supra* note 62 at A13.

70 *Google Spain*, *supra* note 1 at para. 37.

a more significant role ascribed to search engines in information dissemination provides normative justification for a right to be forgotten is a different matter.

III. A 'RIGHT TO BE FORGOTTEN' IN *PIPEDA*?

This section proceeds by analyzing each interpretive step necessary to "discover" a right to be forgotten within *PIPEDA*, based on the discussion in Section 2. At each interval it is assumed that the preceding step is met. For simplicity, and given the fact that Google's share of the Canadian search engine market is nearly 90%,[72] I use Google throughout this section.

(a) Application — *"Collects, uses or discloses. . ."*

The EU Court held that Google's crawling function constituted the "collection" of personal information, and the listing of search results represented "disclosure."[73] Unfortunately, decisions by the Privacy Commissioner and courts under *PIPEDA* have had little reason to scrutinize the definition of "collection, use or disclosure". However, Canadian courts in other contexts have hinted at a limited role for search engines in information dissemination. In *Newton*, the Supreme Court held that a mere hyperlink on the defendant's website to defamatory content could not constitute defamation. Writing for the majority, Justice Abella stated: "A reference to other content is fundamentally different from other acts involved in publication. Referencing on its own *does not involve exerting control* over the content."[74] Moreover, as the defendant's hyperlinking only communicated the *existence* of content, rather than the content itself, the hyperlinking was "ancillary" to the underlying publication.[75]

Newton provides some indication that a court may not ascribe the same role to search engines as the EU Court. Although exercising control over personal information is not a requirement of *PIPEDA per se*, control is closely linked conceptually to the collection, use or disclosure of personal information. Indeed, control is a central organizing principle of *PIPEDA*. Principle 1 of *PIPEDA* states that "[a]n organization is responsible for personal information under its *control*."[76] The control argument would also support Google's position — rejected in *Google Spain* — that by automatically crawling and indexing websites

---

[71] See Muge Fazlioglu, "Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet" (2013) 3:3 International Data Privacy LJ 149 at 152.

[72] "The Webcertain Global Search & Social Report 2014" (2014) at 15, online: <globalcentral.net/assets/cb757434/1403168172_The_Webcertain_Global_Search_-and_Social_Report_Q2_2014.pdf>.

[73] *Google Spain, supra* note 1 at paras. 26-31. As I note in Section 2, the EU Court made no finding regarding the "use" of personal information.

[74] *Newton*, *supra* note 18 at para. 26 (per Abella J) (emphasis added).

[75] *Ibid.*

[76] *PIPEDA*, *supra* note 14 at Sch 1 at s. 4.1 (emphasis added).

without regard to whether the information constituted "personal data", Google could not be processing personal data.[77] In addition, describing hyperlinking as ancillary to publishing suggests that search results may not constitute "disclosure" under *PIPEDA*.

However, caution should be exercised in drawing definitive conclusions from *Newton*. Clearly the focus of the case was on the tort of defamation rather than an interpretation of *PIPEDA*. The court was not asked to inquire into the differences between hyperlinks from one website to another, and hyperlinks from a search engine to a website: hyperlinks in search results are the product of the search engine continuously crawling, indexing and organizing internet content. Nor was the court asked to determine whether search engines *create* content by generating a "structured profile" based on a search of a person's name, and providing a sorting function to internet users. Signals that courts may distinguish search engines from ordinary websites may be found in *Equustek Solutions Inc v Jack,*[78] where the British Columbia Court of Appeal upheld a lower court ruling — also in a different context — that "Google internet search websites are not passive information sites" because, *inter alia*, the search site "collects a wide range of information" including users' IP addresses, location, search terms, and "click-throughs".[79] The court also referred to Google's webcrawling software as an "active process".[80] The Supreme Court granted leave to appeal in this case, potentially offering further guidance on the nature of search engines' activities. I refer to *Equustek* below in more detail in discussing jurisdiction.

(b) Application — *". . . in the course of commercial activities"*

Google generated $55 billion in revenue in 2013, the vast majority of which was derived from its online advertising system that allows advertisers to purchase advertisements associated with specific search terms ("Adwords").[81] The search engine is thus undoubtedly a commercial activity. However, Google may argue that search results are severable by type: because advertisers do not generally associate advertisements with individuals' names, little to no revenue is generated by searches that retrieve personal information.[82] In such searches, Google is not

---

[77] *Google Spain*, *supra* note 1 at para. 22.

[78] *Equustek Solutions Inc. v. Jack*, 2015 BCCA 265, 2015 CarswellBC 1590, 75 B.C.L.R. (5th) 315, [2015] B.C.J. No. 1193 (B.C. C.A.) [Equustek], affirming 2014 BCSC 1063, 2014 CarswellBC 1694, 63 B.C.L.R. (5th) 145, [2014] B.C.J. No. 1190 (B.C. S.C.), leave to appeal allowed 2016 CarswellBC 397, 2016 CarswellBC 398 (S.C.C.) [*Equustek (BCSC)*].

[79] *Equustek (BCCA), supra* note 78 at para. 52 affirming *Equustek (BCSC), supra* note 78 at paras. 48-49.

[80] *Equustek (BCCA), supra* note 78 at para. 54.

[81] Google Inc, "Form 10K — Annual Report 2013" (2013) at 26, online: < https://abc.xyz/investor/pdf/20131231_google_10K.pdf > [*Google 2013*].

[82] Based on multiple searches of names on "Google.ca". It is possible for advertisers to target advertisements based on user names.

seeking to profit but instead delivering on its mission to "organize the world's information and make it universally accessible and useful."[83]

An argument based on distinguishing between commercial and non-commercial components of the search function is difficult to sustain given that search histories and "click throughs" are used to make the search engine more efficient and better-performing for all internet users (i.e., by delivering more relevant results), which subsequently attracts more users and advertisers.[84] The phrase "in the course of" implies that it is not necessary that the search corresponding to an individual's name itself be a commercial activity. Indeed, in a 2009 investigation into Facebook's privacy practices, the Assistant Privacy Commissioner determined that the phrase "in the course of commercial activities" would incorporate the collection, use or disclosure of personal information not directly tied to profit-making where the activities enhance user experiences and encourage continued use, "indirectly contributing to the success of [the organization] as a commercial enterprise".[85]

(c) Jurisdiction

PIPEDA does not specify whether or to what extent the privacy obligations attach to organizations located outside of Canada. The most significant case in this regard is *Lawson*, where the federal court overturned the Privacy Commissioner's determination that *PIPEDA* did not grant her jurisdiction to investigate a US-based company. Harrington J. held that where there was a connection to Canada, the Privacy Commissioner had jurisdiction.[86] Later Privacy Commissioner decisions have elaborated upon the connecting factors between the organization's activities and Canada sufficient to ground jurisdiction, which include the residencies of the parties, and the location of the activity, contract, host server, or end user.[87]

---

[83] *Google 2013*, *supra* note 81 at 25.

[84] In *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)*, 2010 FC 736, 2010 CarswellNat 3689, 2010 CarswellNat 2225, [2010] 3 F.C.R. D-20, [2010] F.C.J. No. 889 (F.C.) [*State Farm*], the Federal Court held that for *PIPEDA* to apply, the "primary activity or conduct" in question must be of a commercial nature. However, the test was only developed to distinguish activities that "support and promote electronic commerce" from other activities such as litigation: see paras 104-105. As search engines are deeply connected to electronic commerce, the *State Farm* test is unlikely to apply.

[85] Assistant Privacy Commissioner of Canada, "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the *Personal Information Protection and Electronic Documents Act*" (PIPEDA Case Summary #2009-008) at para. 12.

[86] *Lawson*, *supra* note 29 at paras. 43, 50.

[87] Office of the Privacy Commissioner of Canada, "Law School Admission Council Investigation" (PIPEDA Case Summary #2008-389) at para. 42. See also Office of the Privacy Commissioner of Canada, "Airline must ensure policies comply with Canadian

On the one hand, Google operates in the United States and likely physically processes and stores data outside of Canada. However, the collection, use or disclosure of personal information relates to Canadian residents; the underlying webpages would likely include Canadian sources; Google clearly targets Canadian internet users (i.e., through Google.ca); and Google sells advertising to Canadian companies, albeit through a subsidiary. Judging by other decisions of the Privacy Commissioner, these connecting factors would be sufficient to establish jurisdiction.[88] For example, in *KLM* the airline was held to be subject to *PIPEDA* because it served the Canadian market, had a website targeting Canadians, and collected information on Canadian passengers in order to provide services.[89]

Furthermore, a recent case involving Google points to a seemingly-expanded legal understanding of jurisdiction over search engines. In *Equustek (BCSC)*, the plaintiff sought an injunction against Google to remove the defendant's website from all Google searches after the defendant continued to unlawfully use the plaintiff's trade secrets to manufacture a competing product.[90] Google challenged the jurisdiction of the British Columbia Supreme Court to make such an order.[91] Fenlon J. held that because Google engaged British Columbia residents through features such as predictive search and various forms of information collection (e.g., location tracking),[92] and sold advertising to British Columbia firms, Google carried on a business in the province — satisfying the "real and substantial" connection test specified by s. 10(h) of the British Columbia *Court Jurisdiction and Proceedings Transfer Act* (*CJPTA*).[93] In coming to this conclusion, Fenlon J. disregarded the legal distinction between Google and Google Canada, finding the two "inextricably linked" through the "Adwords" service.[94]

The British Columbia Court of Appeal upheld the lower court's decision but differed to some extent in its approach to the question of jurisdiction.[95] Groberman J.A. held that s. 10 of the *CJPTA* was not necessary to establish the

---

privacy law" (PIPEDA Report of Findings #2011-002) [*KLM*]; Office of the Privacy Commissioner of Canada, "Cloud Computing — Factsheet" (2011).

88 This view is also consistent with others that have commented on the *Google Spain* decision. See e.g. Geist (2014), *supra* note 59 at B4 (Stating that the EU Court's decision to assume jurisdiction over Google was not "particularly surprising" and that "Canada maintains that its privacy laws apply to organizations outside the country that collect, use or disclose personal information of Canadians").

89 *KLM*, *supra* note 87 at para. 5.

90 *Equustek (BCSC)*, *supra* note 78 at paras. 6-8.

91 *Ibid* at paras. 9, 11.

92 *Ibid* at para. 48.

93 *Court Jurisdiction and Proceedings Transfer Act*, S.B.C. 2003, c. 28.

94 *Equustek*, *supra* note 78 at para. 63.

95 See *Equustek (BCCA)*, *supra* note 78 at para. 43.

court's jurisdiction over the subject matter (''territorial competence'') because the ''facts concerning the violation of trade secrets and of intellectual property rights . . . have a strong connection to the Province.''[96] However, Groberman J.A. relied on Fenlon J.'s findings about Google's business and information collection in British Columbia to ground *in personam* jurisdiction over the company.[97] Groberman J.A. stated that Google's concerns that the decision would leave it governed by courts around the world is a function of ''the world-wide nature of Google's business and not any defect in the law that gives rise to that possibility.''[98]

(d) Substantive obligations and rights

If the threshold tests are met, *PIPEDA* would subject Google to the consent obligation and in addition, to the accuracy and use limitation obligations. This paper proceeds by examining whether these obligations could be interpreted so as to give rise to a right to be forgotten, before turning to how the obligations may be shaped by the constitutional guarantee to freedom of expression.

(i) Consent obligation

As noted in Section 2, Article 7(f) of the Directive provides a balancing test relieving data processors from the consent obligation where the activities advance ''legitimate interests''.[99] No similar balancing test is available under *PIPEDA*, raising significant interpretive challenges as Google would have to remove search results containing personal information for which it does not obtain or sustain consent to collect, use or disclose.

Implied consent — the notion that consent ''may reasonably be inferred from the action or inaction of the individual''[100]— is authorized by *PIPEDA* and is capable of mitigating many of the concerns associated with obtaining *initial* consent to collect, use or disclose personal information, particularly for search results containing non-sensitive personal information.[101] However, the more difficult issue for the purposes of this article is not how a search engine might obtain initial consent, but what happens if consent is withdrawn. *PIPEDA* provides that consent may be withdrawn at any time.[102]

---

96 *Ibid* at para. 41.

97 *Ibid* at para. 51.

98 *Ibid* at para. 56.

99 Directive, *supra* at Art 7(f).

100 Office of the Privacy Commissioner of Canada, ''Determining the appropriate form of consent under the *Personal Information Protection and Electronic Documents Act*'' (2004), online: < https://www.priv.gc.ca/resource/fs-fi/02_05_d_24_e.asp >. See also Austin (2006), *supra* note 19 at 32 (discussing implied consent and *PIPEDA*).

101 See *PIPEDA*, *supra* note 14 at Sch 1, s. 4.3.4.

102 *Ibid* at Sch 1, s. 4.3.8.

Some of the challenges associated with the withdrawal of consent are mitigated by the exemptions to the consent requirement under *PIPEDA*. Where the terms of the exemption are met, consent could not be withdrawn because it is not required in the first place. The relevant exemption is triggered where personal information is publicly available and specified by the regulations. While all information retrieved through Google search is publicly available, only a limited number of classes of information are specified by the regulations. The effect of this exemption is that consent is not required (and could not be withdrawn) for personal information contained in business directories (e.g., links to LinkedIn profiles), disclosed in legal proceedings (e.g., lawsuits or convictions), and appearing in a publication "where the individual has *provided* the information"[103] (e.g., articles containing quotes given by an individual, and possibly links to Facebook profiles or pictures posted by an individual). However, the exemption does not cover all — or even a majority — of the search results that contain personal information. News articles, for example, frequently contain personal information that have not been provided by individuals.[104]

The above analysis suggests *PIPEDA* is poorly suited to the search engine context. For those search results that are not subject to the exemption, the consent obligation could permit individuals to shape their own search results by withdrawing consent to search results with unfavourable information. The outcome could be a right to be forgotten far broader in scope than the version articulated by the EU Court, completely divorced from the privacy objective, and costly in terms of freedom of expression.

This analysis also supports Lisa Austin's characterization of *PIPEDA* as an "all-or-nothing approach": once the threshold test is met, the organization must "comply with all ten principles" even where it "makes sense to require compliance with only a subset of these principles."[105] Austin argues that the impact of this lack of "nuance" is that the Privacy Commissioner or courts may narrowly interpret the threshold question so as not to give rise to the impractical or nonsensical substantive obligations.[106] Indeed, one wonders whether the unintelligible consequences of the consent obligation might influence the threshold determination of whether Google "collects, uses or discloses" personal information.

(ii) The accuracy and use limitation obligations

If the threshold tests are met Google would also be bound to the accuracy and use limitation obligations described in Section 2. Individuals would have a

---

[103] SOR/2001-7 (13 Dec 2001) at s. 1 (emphasis added).

[104] It may also be possible to rely on the exemption for personal information "whose collection is clearly in the interests of the individual and consent cannot be obtained in a timely way" in some cases, but such an approach would seem to stretch a plain reading of the phrase "clearly in the interests of the individual".

[105] Austin (2006), *supra* note 19 at 28.

[106] *Ibid* at 28-29.

corresponding right under *PIPEDA* to challenge Google on the accuracy and completeness of their personal information.[107]

The scope of the accuracy and use limitation obligations are ultimately determined by the purpose ascribed by a Canadian court to Google's collection, use or disclosure of personal information. A broader interpretation of Google's purpose would permit more collection, use or disclosure of information and narrow — or eliminate — a right to be forgotten.

One option would be for a Canadian court to follow the EU Court in ascribing a predominantly economic purpose to Google search. Under this approach, search results that contain out-dated, distortive, or extraneous personal information may not be necessary to meeting Google's economic objective in that they arguably have no impact on Google's advertising sales, market share or ability to channel users to other Google products. In such a case, Google would be under an obligation to cease collecting, using, or disclosing the personal information — i.e., delete the search results. To return to an example cited earlier in the paper, under this analysis the Google search results linking to a teacher's past as an actor in erotic films could be seen as excessive in that they do not advance the company's economic position.

As discussed in the inquiry into whether Google search met the commerciality requirement, an alternative view of Google's search function is that the economic function is only part of the company's broader corporate mission "to organize the world's information."[108] This description implicitly incorporates the use of personal information not only by Google but of internet users that seek personal information for a variety of reasons[109] — who are largely sidelined in the economic perspective. On this broader account, seemingly irrelevant or excessive personal information might be viewed as necessary to Google's purpose of making all information accessible to internet users. Thus the search results containing personal information of the teacher's past are simply a consequence of cataloguing the internet; if internet users do not view the material, it will fade from search results. The key problem with this perspective is that the purpose potentially justifies an *infinite* collection of personal information (subject to *PIPEDA*'s reasonableness test[110]), despite the stated principle in *PIPEDA* in favour of "limiting collection".

This discussion reinforces the point made above that *PIPEDA* is somewhat incongruous to the operations of a search engine. It is difficult to predict how a court might react to this challenge. What is clear, in my view, is that freedom of expression will weigh heavily in defining the scope of the obligations.

---

[107] See *PIPEDA*, *supra* note 14 at Sch 1, s. 4.9.

[108] *Google 2013*, *supra* note 81 at 3.

[109] *PIPEDA* appears to consider the use of personal information by "third parties": See *PIPEDA*, *supra* note 14 at Sch 1, s. 4.6 (not specifying that the purposes for which personal information is to be used applies only to "organizations") and s. 4.6.3 (referring to disclosing information to third parties).

[110] See *PIPEDA, supra* note 14 at s. 5(3).

(iii) Freedom of expression

Section 2(b) of the *Charter* states that "everyone. . .has the freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication."[111] *Charter* jurisprudence establishes that freedom of expression attaches to those activities that convey a meaning,[112] and "protects readers and listeners as well as writers and speakers."[113] Those seeking the protection of s. 2(b) must show that their activity promotes one of three rationales for freedom of expression protections: truth seeking; participation in democratic decision-making; and self-fulfillment and personal autonomy.[114] The recognition under *PIPEDA* of some form of right to be forgotten — whether through the consent obligation or accuracy and use limitation obligations — would undoubtedly infringe s. 2(b): webpage originators whose websites are "delinked" from Google would be impeded from reaching (i.e., conveying meaning to) internet users;[115] internet users would be restricted in the content they could read or view; and, depending on how the court characterizes Google's role in information dissemination, Google would be hindered from providing "structured profiles" on individuals and/or transmitting expressive content to internet users.[116] As rights guaranteed by the *Charter* are not absolute, the key question thus revolves around determining the circumstances, if any, under which a right to be forgotten could be demonstrably justifiable under s. 1.

In *Alberta Privacy Commissioner*, a unanimous Supreme Court struck down Alberta's *Personal Information Protection Act* (*PIPA*)[117] in its entirety on the grounds that it infringed freedom of expression.[118] The Alberta Privacy

---

[111] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c. 11 at s. 2(b) [*Charter*].

[112] See *Irwin Toy Ltd. c. Québec (Procureur général)*, 1989 CarswellQue 115F, 1989 CarswellQue 115, (*sub nom. Irwin Toy Ltd. v. Quebec (Attorney General)*) [1989] 1 S.C.R. 927, [1989] S.C.J. No. 36 (S.C.C.) [*Irwin Toy*].

[113] *R. v. National Post*, 2010 SCC 16, 2010 CarswellOnt 2776, 2010 CarswellOnt 2777, [2010] 1 S.C.R. 477, [2010] S.C.J. No. 16 (S.C.C.) at para. 28.

[114] *Irwin Toy, supra* note 112 at para. 53. See also *Grant v. Torstar Corp.*, 2009 SCC 61, 2009 CarswellOnt 7956, 2009 CarswellOnt 7957, [2009] 3 S.C.R. 640, [2009] S.C.J. No. 61 (S.C.C.) at para. 47 [*Torstar*].

[115] In *Newton*, Abella J advanced a related but more general argument about the relationship between information dissemination and website interconnectivity by declaring that "the Internet cannot, in short, provide access to information without hyperlinks": *Newton*, *supra* note 18 at para. 36.

[116] Even if Google's search engine is characterized as a strictly economic operation, s. 2(b) of the *Charter* protects commercial speech: see *Ford c. Québec (Procureur général)*, 1988 CarswellQue 155, 1988 CarswellQue 155F, (*sub nom. Ford v. Quebec (Attorney General)*) [1988] 2 S.C.R. 712, [1988] S.C.J. No. 88 (S.C.C.) at para. 59.

[117] *Personal Information Protection Act*, R.S.A. 2003, c. P-6.5. The legislation is the provincial equivalent to *PIPEDA*: see Office of the Privacy Commissioner of Canada, "Substantially similar provincial legislation" (2013), online: < https://www.priv.gc.ca/leg_c/legislation/ss_index_e.asp > .

Commissioner had determined that in recording and publicizing individuals that crossed a picket line, the union collected, used and disclosed personal information in breach of *PIPA*.[119] The court held that because the recordings furthered the union's interests in a labour dispute, *PIPA* violated the union's freedom of expression.[120] Although the privacy interests protected by *PIPA* had a "quasi-constitutional" nature rooted in the relationship between "individual autonomy, dignity and privacy" and democracy,[121] the Court found that the legislation was overbroad and disproportionate relative to the impact on the union's freedom of expression in the labour dispute context — which lay at the "core" of s. 2(b) — and thus could not be justified under s. 1 of the *Charter*.[122]

Alberta Privacy Commissioner is not immediately applicable to this inquiry as the Supreme Court distinguished Alberta's *PIPA* from *PIPEDA*: *PIPEDA* is restricted to regulating "commercial activity", whereas *PIPA* established a "general rule".[123] Nevertheless, these cases are instructive for the significant weight they attach to freedom of expression vis-à-vis privacy interests.

In my view, a court could adopt one of two approaches with regards to the relationship between freedom of expression and a right to be forgotten. A court may deem *all* search results containing personal information, and the internet search function generally, to be an essential part of truth-seeking and democratic debate in the information age. This approach would conclude that it is impossible to classify search results by their contribution to truth-seeking and democratic debate, and in fact, attempting to do so would undermine these objectives. An interpretation of *PIPEDA* that gives rise to a right to be forgotten would violate the core of s. 2(b) and be disproportionate to the privacy interests protected. The outcome of this approach would be that no consent or accuracy and use limitation obligations would attach to Google search results.

Alternatively, a court may reason that *PIPEDA* demands a case-by-case analysis of the privacy interests relative to the impact on freedom of expression. Search results associated with a person's name can be sorted by their promotion of truth-seeking and democratic discourse. For example, search results containing links to news articles and other forms of media communication might be considered to *prima facie* further these objectives (there may be exceptions in limited cases). As the Supreme Court stated in *Torstar*, "[p]roductive debate is dependent on the free flow of information [and] the

---

[118] *Alberta Privacy Commissioner*, *supra* note 16 at para. 40.

[119] *Ibid* at para. 4.

[120] *Ibid* at para. 17.

[121] *Ibid* at para. 19.

[122] *Ibid* at para. 28.

[123] *Ibid* at para. 15. But see Privacy Commissioner of Canada, "Factum of the Intervener — In the matter of the Information and Privacy Commissioner and Attorney General of Alberta and United Food And Commercial Workers, Local 401" (2013) at para. 30, online: < https://www.priv.gc.ca/leg_c/factum/01_ufcw_e.asp > (expressing concern about constitutional effect on *PIPEDA* of striking down Alberta's *PIPA*).

vital role of the communications media in providing a vehicle for such debate is explicitly recognized in the text of s. 2(b) itself."[124] But other types of search results may only have minimal benefits for truth-seeking and democratic discourse. In such cases, the sensitivity of the search results may serve to limit the personal autonomy and self-fulfillment of the person subject to the search, undermining the third rationale of freedom of expression.[125] These search results lie outside the core of that protected by s. 2(b), making the infringement proportionate to the quasi-constitutional privacy interests protected by the legislation. Search results that fall into this category might include, for example, material that was posted by an individual, removed, but reproduced without that individual's consent;[126] and social media or internet profile websites.[127] The result of the second approach would be the recognition of a version of a right to be forgotten (through the consent or accuracy and use limitation obligations) that is significantly narrower than that formulated in *Google Spain*.

IV. CONCLUSION

This paper suggests that a right to be forgotten is not as foreign to Canadian law as it may seem.[128] The substantive obligations mandated in *PIPEDA* resemble those in the European Directive and provide a legislative framework for a similar finding in Canada. However, the Supreme Court's determination in *Newton* that website hyperlinks do not constitute control over content suggests that Canadian courts may reject the EU Court's assertion in *Google Spain* that search engines "collect" or "disclose" personal information. Moreover, the impractical consequences of finding that *PIPEDA* applies to Google may lead a court to dismiss a claim at the threshold stage. Finally, the right to be forgotten would likely be significantly narrowed — if not defeated — by the Supreme Court's emphasis on freedom of expression relative to privacy rights, as seen in *Alberta Privacy Commissioner*.

This paper has also demonstrated that the privacy frameworks are not particularly well-suited to technologies that process personal information in non-traditional ways. This is not surprising given the Directive was implemented in

---

[124] *Torstar*, *supra* note 114 at para. 51.

[125] See *ibid*.

[126] See Google Inc., "European privacy requests for search removals: Examples of requests we encounter", online: <https://www.google.com/transparencyreport/removals/europeprivacy>; Toobin, *supra* note 13.

[127] See Google Inc., "European privacy requests for search removals: Sites that are most impacted", online: <https://www.google.com/transparencyreport/removals/europe-privacy>.

[128] Others have made broadly similar arguments in contrasting US and European privacy laws. See generally Alessandro Mantelero, "The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'" (2013) 29:3 Computer Law & Security Review 229; Steven C. Bennett, "The 'Right to Be Forgotten': Reconciling EU and US Perspectives" (2012) 30:1 Berkeley J Int'l Law 161.

1995, *PIPEDA* in 2001, and both reflect Fair Information Practices developed in the late 1970s. The consent-based model and the "all-or-nothing" approach of *PIPEDA* in particular leads to significant interpretive challenges that may actually undermine privacy rights.

Responding to the impact of rapid technological change on privacy, in April 2016 the European Parliament enacted a new Directive.[129] Article 17 of the Directive expressly enshrines a right to be forgotten. It remains unclear whether the new Directive will trigger changes globally. At this point, the only certainty is a continued vigorous debate over the right to be forgotten.

---

[129] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ, L 119.

Appendix
Table 1 — Comparison of European and Canadian privacy statutes

Directive 95/46/EC (European Union)	***PIPEDA* (Canada)**
Threshold questions — applicability and jurisdiction	
"Personal data": "any information relating to an identified or identifiable natural person. . ."[Art. 2(a)]	"Personal information": "information about an identifiable individual, but does not include the name, title or business address or telephone number of an organization" [s. 2]
"Processing of personal data": "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction. [Art. 2(b)]	"Applies to every organization in respect of personal information that . . . collects, uses or discloses in the course of commercial activities" [s. 4(1)(a)] "Commercial activity": "any particular transaction, act or conduct or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists" [s. 2]
"This Directive shall apply to the processing of personal data wholly or partly by automatic means. . ." [Art. 3(1)]	
"Controller": legal person. . .which alone or jointly with others determines the purposes and means of the processing of personal data. . ." [Art. 2(c)]	"organization" includes an association, a partnership, a person and a trade union [s. 2]
"Each Member State shall apply [the Directive] to the processing of personal data where. . . the processing is carried out in the context of activities of an establishment of the controller on the territory of the Member State" [Art. 4(1)(a)]	

Directive 95/46/EC (European Union)	***PIPEDA* (Canada)**
"Member States shall provide for exemptions or derogations . . . for the processing of personal data carried out solely for journalistic purposes or for the purpose of artistic or literary expression only if they are necessary to reconcile the right to privacy with the rules governing freedom of expression" [Art 9]	"This Part does not apply to. . .any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose" [Art. 4(1)(c)]
Substantial obligations and rights	
"Personal data may be processed [without consent of the data subject] only if . . . processing is necessary for the purposes of the legitimate interests pursued by the controller. . .except where such interests are overridden by the interests [or] fundamental rights and freedoms of the data subject. . ." [Art. 7(f)]	"The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate" [Sch. 1, s. 4.3] "an organization may collect personal information without the knowledge of consent of the individual only if. . . the information is publicly available and is specified by the regulations [s. 7(1)]
Personal data "must be adequate, relevant and not excessive in relation to the purposes for which they are collected" and "accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected. . .are erased and rectified" [Art. 6(d)]	"Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used" [Sch. 1, s. 4.6] "The collection of information shall be limited to that which is necessary for the purposes identified by the organization." [Sch. 1, s. 4.4]
	"Personal information shall not be used or disclosed for purposes other than those for which it was collected. . .Personal information shall be retained only as long as necessary for the fulfillment of those purposes." [Sch. 1, s. 4.5]
	"Organizations shall not collect personal information indiscriminately" [Sch. 1, s. 4.4]

Directive 95/46/EC (European Union)	***PIPEDA* (Canada)**
	"An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances" [s. 5(3)]
"A right to obtain from the controller. . .as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" (Art. 12)	"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" [Sch 1, s. 4.9.5]
"Member states shall grant the data subject the right. . .at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation" [Art 14]	"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" [Sch. 1, s. 4.9]