Privacy above all other Fundamental Rights?

Challenges with the Implementation of a Right to be Forgotten in Canada*

Eloïse Gratton and Jules Polonetsky*****

Executive Summary

This paper explores whether importing a "right to be forgotten" (RTBF) that would allow individuals to stop data search engines or other third parties, from providing links to information deemed irrelevant, no longer relevant, inadequate or excessive would be advisable in Canada. The authors argue that not only such a right would be unconstitutional in Canada but also that such RTBF may be, in any event, unnecessary and undesirable both from a legal and a public policy perspective. The authors first argue that a RBTF would most likely infringe upon freedom of expression in a way that cannot be demonstrably justified under the Canadian Constitution. Second, they argue that the current legal framework in place in Canada, at least in some provinces, efficiently addresses the privacy and reputational concerns that a RTBF is meant to address. Finally, the authors raise concerns about the risks pertaining to the RTBF, most notably with respect to the restrictions on the flow of information, as well as the negative impact the implementation of a RTBF has had in Europe over recent months. In their conclusion, the authors warn against entrusting private entities with the tasks of arbitrating fundamental rights and values and determining what is in the public interest, with little or no government or judicial oversight. They suggest, instead, that efforts be put into improving the current legal framework, notably by increasing access to justice, rather than by importing a RTBF that would prove to be inefficient and, to some extent, counterproductive.

* This paper dated April 28, 2016, is submitted to the Office of the Privacy Commissioner of Canada, as part of its Consultation and Call for Essays on Online Reputation. We are grateful for the valuable contribution from attorney Patrick Plante, articling student Raphaël Girard and student at law Julien Boudreault with Borden Ladner Gervais LLP, as well as Laura Vivet, EU Fellow with the Future of Privacy Forum.

** Partner and National Co-Leader, Privacy and Data Security Practice Group of Borden Ladner Gervais LLP. The content from this white paper should not be understood or considered as providing legal advice. The views expressed herein are solely those of the author in her private capacity and do not in any way represent the views of the law firm Borden Ladner Gervais LLP.

***Executive Director and Co-chair, Future of Privacy Forum.

TABLE OF CONTENTS

INTRODUCTION

The Internet has enabled anyone to access almost all the knowledge that exists today. By using search tools critical information is available to students, researchers, reporters or consumers seeking content they need. The leading way users today find information is via links they find on social media or via searches. While access to data offers significant social benefits, it also carries risks to individuals. False information can be published and true but derogatory information may be maintained long after it is relevant.

In response to these risks, European policymakers have proposed legislation recognizing a "right to be forgotten" (hereinafter "RTBF"). The latter would provide individuals in European Union countries with a legal mechanism to compel the removal of their personal information from online databases. More specifically, while the European Directive 95/46/EC already includes the principle underpinning the RTBF,[1] the forthcoming data Regulation specifically includes an article entitled "Right to Erasure."[2] In May 2014, the Court of Justice of the European Union (CJEU), exercising jurisdiction over twenty-eight E.U. member states, issued a landmark decision in *Google Inc. v. Agencia Española de Protección de Datos* ("CJEU Case" or "Google Spain" case).[3] In this case, Mario Costeja González, a Spanish lawyer, had been in debt. When some of his property was auctioned, a local newspaper, *La Vanguardia*, published two small notices announcing the auction in 1998. By 2010, Costejahad resolved his debts and realized that Google searches under his name linked him with the old news article. He sued, petitioning a Spanish court to order deletion of the record of the auction as to both *La Vanguardia*'s publication and Google's linking the same to Costeja,[4] claiming that he had a "right to be forgotten", and that the auction notice was no longer "relevant."[5] The Spanish court referred the case to the CJEU certifying three legal issues, the third of which asked "whether an individual has a right to request that his or her personal data be removed from accessibility via a search engine (the 'right to be forgotten')."[6] The CJEU held that the auction publications could remain on the newspaper's website, but mandated Google to delete any link connecting Costeja to them.

According to many, the CJEU in this case pronounced a broad precedent: all European residents now have the right to stop Google and other *data controllers* from linking to information deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they

---

[1] See European Commission, "Factsheet on the 'Right to be Forgotten' Ruling", online: < http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf> [European Commission, "Factsheet"]. Support for the claim that the Directive includes the RTBF stems from Article 12 of the Directive 95/46/EC, of the European Parliament and of the Council of October 24, 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 [Directive 95/46/EC].

[2] European Commission, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, COM (2012) 11 final, article 17 [General Data Protection Regulation].

[3] *Google Spain SL* v. *Agencia Española de Protección de Datos*, Case C-131/12 (May 13, 2014), online: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=363285> [*Google Spain SL*].

[4] *Ibid*, at para. 14.

[5] *Ibid*; see also Dave Lee, "What Is the 'Right To Be Forgotten'?", *BBC News* (13 May 2014) online: <http://www.bbc.com/news/technology-27394751>.

[6] *Google Spain SL*, *supra* note 3, at 18-20; See also European Commission, "Factsheet", *supra* note 1.

were processed and in light of the time that had elapsed."[7] Some are warning that the standard to determine if such information should be removed lacks objective guideposts, and moreover, that it is unclear what notification (if any) Google must give to websites and others that their links have been erased.[8] One U.S. commentator has even claimed that "this decision will go down in history as one of the most significant mistakes that court ever made."[9] Others are welcoming this new right to be forgotten, considering it as a way for individuals to better protect their online reputations.[10] As of the writing of this paper, Google has reported[11] receiving over 405,305 take-down requests, covering over 1.4 million URLs. Google has confirmed that it removes hyperlinks in about 42% of such cases.[12]

The lack of consensus on the relevancy of a RTBF illustrates, to a certain extent, the cultural transatlantic clash on the issue of the importance of privacy versus other rights, such as freedom of information and freedom of speech. Some commentators have argued that the Americans' unilateral protection of freedom of the press under the First Amendment can be opposed to the Europeans' inclusion of a countervailing right to personality in the European *Convention on Human Rights* Article 8. Indeed, as explained by Professor Werro on one side of the spectrum, the Americans put great faith in the private sector, which translates into a general preference for market self-regulation, while Europeans, one the other side of the spectrum, have trust in the government and share a common distrust vis-à-vis the market. [13] The end result of these diametrically opposed views is if while Americans will be ready to relinquish some of their privacy in order to protect the flow of information and increase the availability of information, Europeans will prefer a shutting off of the flow of information to the institution that they trust the least, namely the market.[14]

Canada, on the issue of freedom of information, freedom of expression vs. privacy, sits somewhere in the middle. While freedom of expression is protected by the Canadian Constitution, privacy is also valued. For instance, Canada has data protection laws which are similar to the European Directive 95/46/EC. Within Canada, Quebec, a primarily French-speaking province, has the most stringent privacy

---

[7] *Ibid*, at para. 94.

[8] Robert Peston, "Why has Google Cast me into Oblivion?", *BBC News* (2 July 2014) online: <http://www.bbc.com/news/business-28130581>; See also McKay Cunningham, "Free Expression, Privacy and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship" (2015) Arkansas Law Review [forthcoming], at 4 [Cunningham, "The Internationalization of Censorship"].

[9] Jeffrey Toobin, "The Solace of Oblivion - In Europe, the right to be forgotten trumps the Internet", *The New Yorker* (29 September 2014) online: <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion>.

[10] Frank A. Pasquale, *Reforming the Law of Reputation* (2015), 47 Loyola University Chicago Law Journal 515 (2015); U of Maryland Legal Studies Research Paper No. 2016-03 [Pasquale]; Paulan Korenhof and Ludo Gorzeman, *Who is Censoring Whom? An Enquiry into the Right to be Forgotten and Censorship* (July 2015), online at: <http://dx.doi.org/10.2139/ssrn.2685105>

[11] See Google, "Transparency Report: European Privacy Requests for Search Removals" (17 March 2016), online: Google <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en-US> [Google, "Transparency Report"].

[12] Google, "Letter from Google to the Article 29 Working Party" (31 July 2014), online: <https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit?pli=1> [Google, "Letter from Google to the Article 29 Working Party"]

[13] Franz Werro, "The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash" in Aurelia Colombi Ciacchi, Christine Godt, Peter Rott and Leslie Jane Smith, eds, *Liability in the Third Millennium* (Baden-Baden: Nomos, 2009), online: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357>, at 298.

[14] *Ibid.*

regime and reputational legal framework; Quebec could, in some ways, be considered as the "California" of Canada.

The Office of the Privacy Commissioner of Canada ("OPC") has, in 2015, chosen reputation and privacy as one of its priorities for the next five years. The OPC is focusing its attention on the reputational risks stemming from the vast amount of personal information posted online and on existing and potential mechanisms for managing those risks. In January 2016, the OPC published a discussion paper, entitled "Online Reputation, What are they saying about me?", in which it asks if the RTBF can find application in the Canadian context and if so, how.[15]

This paper is meant to provide an answer to this question. More specifically, the paper will first discuss the constitutional challenges with the implementation of a RTBF in Canada (section 1). It will then elaborate on the current legal framework already in place in Canada and which may, to a certain extent, address some of the concerns which are meant to be addressed through a RTBF, in order to determine whether we need such a right in Canada (section 2). Lastly, this paper will discuss the risks pertaining to the RTBF, most notably in terms of outsourcing the balancing of important rights to a private corporation, infringements on freedom of expression, as well as the negative impact the implementation of the RTBF has had in Europe in recent months (section 3).

[15] Policy and Research Group of the Office of the Privacy Commissioner of Canada, "Online Reputation, What are they saying about me?" (Discussion Paper, Office of the Privacy Commissioner of Canada, 2016) online: <https://www.priv.gc.ca/information/research-recherche/2016/or_201601_e.asp>, at 13 ["Online Reputation, What are they saying about me?"].

1. CONSTITUTIONAL CHALLENGES WITH RTBF IN CANADA

At first sight, the recognition in Canada of a RTBF does not sound that far-fetched. In fact, Canadian data protection laws are modelled on European standards[16] and it seems plausible that a Canadian court could, to a certain extent, interpret them as granting such a right, as the Court of Justice of the European Union did in the *Google Spain* decision[17] applying Directive 95/46/EC.[18] In addition, Canadian legislatures might be tempted to follow the European example and to respond to concerns about Internet privacy by legislating to confer upon individuals a right to request that certain personal information be deindexed from search engine results when certain conditions are met.[19]

This begs the question of whether such judicial interpretation of existing statutes or legislative initiatives would be consistent with the Constitution of Canada. As is the case with the U.S. Constitution, the Canadian Constitution explicitly protects freedom of expression, while omitting any specific and comprehensive right to privacy in which a RTBF could be anchored. In all likelihood, search engine results would be considered by Canadian courts as "expressions" worthy of constitutional protection.

Does this mean that the very idea of a Canadian RTBF is doomed from the outset? Although it is difficult to predict how Canadian courts would rule on this issue, we believe that the approach adopted in Europe would likely be considered unconstitutional. While Canadian constitutional law allows for reasonable limitations of fundamental rights, a European-style RTBF could hardly be justified under the criteria adopted by Canadian courts. In our view, it fails to strike an appropriate balance between freedom of expression and privacy.

Furthermore, we believe that private corporations are not the adequate forums to address the fundamental issues at stake. There are reasons to be wary of entrusting private corporations with the duty to rule – based on subjective criteria – on the rights of third parties without them having a chance to intervene and to be heard, and with little or no public oversight. Such a secretive process seems poised to favour the removal of information, to the detriment of freedom of expression and this issue is further discussed in section 3.1.

In examining the constitutionality of a hypothetical Canadian RTBF, this section will review: the constitutional status of rights and freedoms in Canada (section 1.1) the scope of freedom of expression (sections 1.2), as well as the appropriate balance between such a fundamental right and privacy under the Canadian constitutional framework (section 1.3).

1.1 Rights and freedoms in Canada

The constitutional entrenchment of civil liberties is of a rather recent date in Canadian history. Originally, when North American British colonies federated in 1867 to create the Dominion of Canada, the drafters of the constitution had chosen not to follow the American example and rejected the idea of

[16] Eloïse Gratton, *Understanding Personal Information, Managing Privacy Risks* (Markham: LexisNexis, 2013), at 14-21.

[17] *Google Spain SL*, *supra* note 3.

[18] *Supra* note 1.

[19] Some Canadian lawyers and scholars are calling for a reform of data protection laws in order to introduce a "right to be forgotten". See e.g. Geneviève Saint-Laurent, "Vie privée et « droit à l'oubli »: Que fait le Canada?" (2015) 66 UNBLJ 185, at 185-186 and 196.

including a bill of rights.[20] The protection of rights and freedoms was left to the common law and to ordinary statutes,[21] always subject to parliamentary sovereignty.[22] This changed dramatically in 1982 with the enactment of the *Canadian Charter of Rights and Freedoms* (the "Charter"),[23] which is now the Canadian counterpart of the American Bill of Rights.

1.1.1 The Canadian Charter of Rights and Freedoms

As part of the formal Constitution of Canada, the Charter can only be changed through complex – and politically sensitive – amending procedures, thus ensuring that guaranteed rights and freedoms will not be abrogated by ordinary legislative action.[24] The Charter applies to all levels of government, but not directly to private activity.[25] Due to its supreme status, it overrides any inconsistent federal or provincial law, effectively providing a basis for judicial review of legislation and regulations which curtail civil liberties.[26] This has led the courts to play an increasingly important role with regard to the most pressing social and political issues in Canada.

The Charter gives constitutional protection to, *inter alia*, fundamental freedoms, such as expression, at section 2(b), and to legal rights, such as the right not to be deprived of life, liberty and security – except in accordance with the principles of fundamental justice[27] – at section 7, and the right to be secure against unreasonable search or seizure, at section 8. Of particular note is that the Charter does not specifically protect the right to privacy, in contrast to the *Charter of Fundamental Rights of the European Union*[28] and the *European Convention on Human Rights.*[29] Nonetheless, as is the case with the U.S. Constitution,[30] Canadian courts have inferred from the legal rights declared in the Charter a limited right

[20] See the *Constitution Act*, 1867, 30 & 31 Vict, c. 3.

[21] Ordinary statutes that protect civil liberties include the *Canadian Bill of Rights*, SC 1960, c. 44, which was adopted in 1960 with little effect. See Peter W. Hogg, *Constitutional Law of Canada*, loose-leaf (consulted on 2 March 2016), 5th ed. suppl. (Toronto, Ont.: Carswell, 2007), at 35-10-11.

[22] It should be noted though that the Supreme Court of Canada had sometimes read into the *Constitution Act* of 1867 an *implied* right to freedom of expression, which was deemed to be essential to the parliamentary regime provided for by the constitutional text. See Hogg, *Constitutional Law of Canada*, *supra* note 21, at 1-6 and 34-2 to 36-2.

[23] *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. The *Canada Act 1982* is the British statute which put an end to the authority of the United Kingdom Parliament over Canada.

[24] See s. 52 (3) of the Charter.

[25] See s. 32 of the Charter. There is still ample debate and confusion about the reach of the Charter, especially with respect to government action. What is the proper definition of "government" within the meaning of the Charter? For our purposes, suffice it to say that the Charter will generally apply to organizations which are subject to a substantial level of government control. See Hogg, *Constitutional Law of Canada*, *supra* note 21, at 37-18-19.

[26] See Hogg, *Constitutional Law of Canada*, *supra* note 21, at 1.12-1, 36-3 and 36-5. Before the enactment of the Canadian Charter, constitutional control was limited to issues pertaining to the federal-provincial distribution of powers.

[27] "Principles of fundamental justice" replace the notion of "due process" found in the American Fifth Amendment.

[28] European Union, *Charter of Fundamental Rights of the European Union*, 26 October 2012, 2012/C 326/02, s. 7-8.

[29] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, 4 November 1950, ETS 5, s. 8.

[30] McKay Cunningham, "Diminishing Sovereignty: How European Privacy Law Became International Norm" (2013) 11 Santa Clara Int'l L 421, 443.

to a reasonable expectation of privacy, especially from state intrusion,[31] and have recognized privacy as a "fundamental value that lies at the heart of a democracy".[32]

Courts are often called upon to intervene when Charter rights collide with each other or with non-Charter values.[33] As opposed to its American equivalent, the text of the Canadian Charter offers some guidance as to how to solve such conflicts. The very first section of the Charter provides that guaranteed rights and freedoms are "subject to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society". Section 1 of the Charter makes it clear that constitutional rights and freedoms are not absolute and that, in certain circumstances, they can be restrained in order to pursue collective goals of fundamental importance.[34]

With respect to judicial review, these principles translate into a two-step process by which courts first decide whether the law infringes one of the Charter rights and, if so, analyze whether such infringement is justified under section 1 of the Charter.[35] This process applies to impugned statutes, regulations and other enactments of general application.[36]

The onus is always on the claimant to establish that the law encroaches upon one of his or her Charter rights. This generally involves interpreting the relevant provisions of the Charter to define the scope of the rights at stake and to determine whether the activity of the claimant falls within the protected sphere of conduct.[37] Once the Charter violation is established, the burden rests on the government (or any other party seeking to uphold the law) to demonstrate, on a balance of probabilities, that the limitation is justified under section 1 of the Charter. In this regard, the Supreme Court of Canada has set out, in the seminal *Oakes*[38] decision, a fourfold test: 1) the law pursues a pressing and substantial objective; 2) the means are rationally connected to this objective; 3) the law impairs the right no more than necessary to accomplish its objective; and 4) the deleterious effects of the law are not disproportionate to its benefits.[39]

---

[31] More specifically, a limited right to privacy has been found to derive from s. 7 ("life, liberty and security") and from s. 8 (protection against "unreasonable search and seizure") of the Charter. See e.g. *Hunter* v. *Southam Inc*., [1984] 2 SCR 145, at para. 25; and *R*. c. *O'Connor*, [1995] 4 SCR 411, at para. 110-119 (concurring opinion of J. L'Heureux-Dubé). See also Michael Power, *The Law of Privacy* (Markham: LexisNexis, 2013), at 231-252.

[32] *Alberta (Information and Privacy Commissioner)* v. *United Food and Commercial Workers, Local 401*, 2013 SCC 62, at para. 19 [*UFCW*].

[33] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 36-12.

[34] *R*. v. *Oakes*, [1986] 1 SCR 103, at 136 [*Oakes*].

[35] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-2-3.

[36] The Charter equally applies to individual government decisions, though the justification of such decisions will not generally be reviewed through the framework set forth in s. 1 of the Charter. Courts will simply assess whether the decision-maker has taken sufficient account of Charter values, considering the specific facts of the case, in exercising its discretionary power. See *Doré* v. *Barreau du Québec*, [2012] 1 SCR 395, 2012 SCC 12, at para. 36-55. See also Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-13-14.

[37] See Hogg, *Constitutional Law of Canada*, at 38-7. See also *Irwin Toy Ltd*. v. *Quebec (Attorney General)*, [1989] 1 SCR 927, at 967-968.

[38] *Oakes*, *supra* note 34, at 138-140.

[39] See Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-17-18.

If the infringement does not pass the so-called "*Oakes* test", the law will generally be held to be unconstitutional and invalid (in whole or in part). Alternatively, when there is ambiguity about the meaning of the challenged provisions, courts may adopt a narrow interpretation so as to avoid a breach of the Charter.[40]

As a basic principle, the Charter does not apply to the common law as it pertains to the relationships between private parties. The Supreme Court of Canada has, however, significantly qualified that principle, by asserting that the judiciary ought to develop and alter the common law in a manner consistent with the values underlying the Charter.[41] For instance, this led the court to modify the tort of defamation, giving greater weight to the freedom of expression.[42] In such cases, the courts will not apply the limitation test of section 1 of the Charter, but will rather balance the values at stake through a more flexible approach.

1.1.2 Statutes Protecting Freedom of Expression and Privacy

Apart from the Canadian Charter, three provinces have enacted statutory bills of rights,[43] which guarantee a wide range of rights and freedoms, including freedom of expression. These statutes are deemed **"**quasi-constitutional", in that they have priority over inconsistent provincial laws, making the latter inoperative.[44] However, unlike the Canadian Charter, these bills of rights are subject to ordinary legislative amendment or abrogation.

Among such provincial legislation, Quebec's *Charter of Human Rights and Freedoms* (the "Quebec Charter") is unique in guaranteeing everyone the "right to respect for his private life".[45] Under the Quebec Charter, any unlawful infringement of a protected right may entitle the victim to an injunction

---

[40] *Ibid*, at 40-3-4; Pierre-André Côté, *The Interpretation of Legislation in Canada*, 4th ed. (Toronto, Ont.: Carswell, 2011), at 498 and 499. For an example pertaining to freedom of expression, see *Canada (Attorney General)* v. *JTI-Macdonald Corp*., [2007] 2 SCR 610, 2007 SCC 30, at para. 52-57. It should be noted that the justification criteria of section 1 are not the only means through which a government can uphold limitations to Charter rights. Section 33 of the Charter enables legislatures to override most rights – including freedom of expression – by declaring in a statute that the whole act or some of its provisions may operate notwithstanding the Charter. Such a declaration immunizes the statute from challenges on Charter grounds, without the need for justification. In practice, however, the so-called "notwithstanding clause" has never been used by the federal Parliament and seldom by most provinces. It is generally believed that its use would be met with strong political opposition. On this issue, see Hogg, *Constitutional Law of Canada*, *supra* note 21, at 39-2-3, 39-9.

[41] See *RWDSU* v. *Dolphin Delivery Ltd*, [1986] 2 SCR 573, at 603; *Hill* v. *Church of Scientology of Toronto*, [1995] 2 SCR 1130, at para. 91-98 [*Hill*].

[42] *Grant* v. *Torstar Corp*., 2009 SCC 61, at para. 38-65 [*Torstar*].

[43] *Saskatchewan Human Rights Code*, SS 1979, c. S-24.1; *Alberta Bill of Rights*, RSA 2000, c. A-14; Quebec's *Charter of Human Rights and Freedoms*, CQLR, c. C-12. The federal Parliament and provincial legislatures have also adopted human rights codes to promote equality rights and fight against discrimination, especially in employment and accommodation. These statutes apply to the private sector. Under certain circumstances, they may prevent personal information from being collected or used for discriminatory purposes. See also section 2.1.2 of this paper, which further discusses these bills.

[44] See s. 44 of the *Saskatchewan Human Rights Code*, s. 2 of the *Alberta Bill of Rights* and s. 52 of the Quebec Charter. In balancing conflicting rights, Quebec courts apply section 9.1 of the Quebec Charter, which is the equivalent of s. 1 of the Canadian Charter.

[45] See s. 4-5 of the Quebec Charter. With respect to the scope of the right to privacy under the Quebec Charter, it is worth mentioning *Aubry* v. *Éditions Vice-Versa inc*., [1998] 1 SCR 591 [*Aubry*], where the Supreme Court of Canada held a photographer liable for taking and publishing a picture of a teenage girl, sitting on the steps of a building, without her consent. In that particular case, the Court reached the conclusion that the girl's right to privacy outweighed the artist's freedom of expression. The photographer and its publisher were ordered to pay $2000 in damages.

or to damages.[46] As further discussed in section 2, since the Quebec Charter applies to private persons, an individual could, in our view and under certain circumstances, rely on his or her right to privacy to claim a RTBF, by seeking an injunction against a search engine operator.[47] Before granting any such relief, the court would then have to take into account the value of freedom of expression, which is also guaranteed by the Quebec Charter.

All across the country, federal Parliament and provincial legislatures alike have enacted data protection laws in both the public and private sector.[48] The Supreme Court of Canada has stated that these statutes should be characterized as "quasi-constitutional", because of the fundamental role privacy plays in the preservation of a free and democratic society.[49] As mentioned before, the language of those statutes is inspired by European legislation and, as such, could arguably be construed so as to confer a RTBF, although these laws also have their limits and challenges, as further discussed in section 2.1.2.[50] Moreover, as further discussed in section 2, some common law provinces have enacted legislation providing a right of action for breach of privacy.[51] In Ontario, for example, courts have recently recognized privacy torts under the common law.[52] Such common law torts apply only in cases of "highly offensive" violations in matters not of legitimate concern to the public.[53]

1.2 The Scope of Freedom of Expression

Section 2(b) of the Canadian Charter provides that everyone has the fundamental freedom of expression, including freedom of the press and other media of communication. The Charter is subject to

[46] See s. 49 of the Quebec Charter.

[47] In Quebec, a limited RTBF could equally arise from sections 35 and 36(5) of the *Civil Code of Quebec*, CQLR, c. C-1991, which contemplate that using the name of a person for any other purpose than the "legitimate information of the public" amounts to an invasion of privacy. See section 2.2.1 of this paper which further discusses this legal framework.

[48] See section 2.1.1 of this paper which further discusses this legal framework for the private sector. As a matter of example, see the federal *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5. In terms of constitutional distribution of powers, suffice it to say that federal and provincial governments have concurrent jurisdiction in matters of privacy. See Power, *The Law of Privacy*, *supra* note 31, at 11-12.

[49] *Lavigne* v. *Canada (Office of the Commissioner of Official Languages)*, 2002 SCC 53, at para. 24-26; *UFCW*, *supra* note 32, at para. 19.

[50] See also Andre Mayer, "*Right to be forgotten: How Canada could adopt similar law for online privacy*", *CBC News* (16 June 2014) online: <http://www.cbc.ca/news/technology/right-to-be-forgotten-how-canada-could-adopt-similar-law-for-online-privacy-1.2676880>.

[51] British Columbia *Privacy Act*, RSBC 1996, c. 373; Manitoba *Privacy Act*, CCSM, c. P125; Newfoundland and Labrador *Privacy Act*, RSNL 1990, c. P-22; and Saskatchewan *Privacy Act*, RSS 1978, c. P-24.

[52] See *Doe 464533* v. *N.D.*, 2016 ONSC 541 [*Doe 464533*] (public disclosure of embarrassing private facts) and *Jones* v. *Tsige*, 2012 ONCA 32 [*Jones* v. *Tsige*] (intrusion upon seclusion).

[53] See e.g. *Doe 464533*, *supra* note 52, at para. 36, 46-47. In light of the recent recognition of privacy torts by Ontario courts, some authors have suggested that a right to be forgotten could take root within the common law. See Mike Wagner and Yun Li-Reilly, "The Right to Be Forgotten" (2014), 72 Advocate Vancouver 823, at 825. In our view, such a development of the common law is very unlikely considering that the new torts only provide a right of action in cases of "highly offensive" violations, such as intrusions into one's financial or health records, sexual practises and orientation, employment, diary or private correspondence. See *Jones* v. *Tsige*, *supra* note 52, at para. 72-73. That being said, it is worth mentioning that the Court of Appeal for British Columbia has granted an injunction prohibiting Google from delivering search results pointing to the website of a business which infringed the intellectual property of the plaintiff: *Equustek Solutions Inc.* v. *Google Inc.*, 2015 BCCA 265 [*Equustek*]. Such an injunction might arguably be granted in a case of invasion of privacy. In any event, it would be a very limited – and judicially enforced – "RTBF".

a "purposive" and "generous" interpretation, which is meant to give full effect to the civil liberties that it guarantees.[54] Freedom of expression is no exception. The notion of "expression" has been construed very broadly, so as to include any activity that attempts to convey meaning, including both form and content.[55]

Competing Charter rights and values cannot curtail the scope of freedom of expression *per se*. For instance, with regard to hate propaganda, the Supreme Court of Canada has rejected the idea of narrowing the protection afforded by section 2(b) by reference to equality rights.[56] Any rights or values that collide with freedom of expression must be analysed under the Charter's section 1 inquiry, to determine whether they justify a limitation in specific circumstances.

Where government purports to ban particular meanings or to restrict the ability to convey or access such meanings, freedom of expression is deemed to be infringed, irrespective of the actual content that is targeted.[57] This is because the Supreme Court of Canada has adopted the principle of content neutrality, which provides that "the content of a statement cannot deprive it of the protection accorded by s. 2(b), no matter how offensive it may be".[58] In light of this principle, commercial advertisement is undeniably worthy of constitutional protection.[59] Even content such as false news,[60] hate speech[61] and pornography[62] cannot be excluded from the reach of section 2(b).[63] Violent acts, however, do fall outside the scope of freedom of expression.[64]

The Supreme Court of Canada has recognized that freedom of expression is essential to the functioning of our democracy, to seeking the truth in diverse fields of inquiry, and to our capacity for self-expression

---

[54] *R.* v. *Big M Drug Mart Ltd*., [1985] 1 SCR 295, at 344.

[55] *Irwin Toy Ltd*., *supra* note 37, at 968-969. In this decision, the Supreme Court of Canada gave the example of "parking" as an activity that could be protected if used to convey meaning, such as for protesting against a by-law.

[56] *R*. c. *Keegstra*, [1990] 3 RCS 697, at 733-734 [*Keegstra*].

[57] *Irwin Toy Ltd*., *supra* note 37, at 974, where the Supreme Court of Canada held that a prohibition of advertising aimed at children infringes freedom of expression but may be justified under s. 1 of the Charter.

[58] *Keegstra*, *supra* note 56, at 828.

[59] *Ford* v. *Quebec (Attorney General)*, [1988] 2 SCR 712, at 766-767 [*Ford*], where the Supreme Court of Canada struck down Quebec's language legislation that required commercial signs to be solely in French. See also *RJR-MacDonald Inc*. v. *Canada (Attorney General)*, [1995] 3 SCR 199, where the Supreme Court of Canada held that the requirement that tobacco manufacturers place an unattributed health warning on packages infringed freedom of expression and could not be justified under s. 1 of the Charter. However, in *Canada (Attorney General)* v. *JTI-Macdonald Corp*., 2007 SCC 30, the Supreme Court of Canada upheld an anti-tobacco law which required tobacco manufacturers to place a warning attributed to the government on their products.

[60] *R*. v. *Zundel*, [1992] 2 SCR 731 [*Zundel*].

[61] *Saskatchewan (Human Rights Commission)* v. *Whatcott*, 2013 SCC 11 [*Whatcott*].

[62] *R*. v. *Butler*, [1992] 1 SCR 452. See also *R*. c. *Sharpe*, 2001 CSC 2, at 242, where the Supreme Court of Canada held that child pornography offences infringe freedom of expression but may be justified under s. 1 of the Charter. In order to mitigate the restriction of expressive activities, the Court interpreted the *Criminal Code* so as to carve out an exception for written material or visual representations created by the accused alone for his personal use.

[63] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 43-31-39.

[64] *Keegstra*, *supra* note 56, at 731.

and individual realization.[65] As such, public interest has been construed broadly so as to include matters ranging from "politics to restaurant and book reviews".[66]

The core purposes of freedom of expression – democratic discourse, truth-seeking and self-fulfillment – should be taken into account under section 1 of the Charter to assess whether an infringement is justified. It goes without saying that content of dubious value, such as racial propaganda, will invite lower standards of justification.[67] On the contrary, when core purposes are involved, freedom of expression will be given greater weight.

Canadian courts have shown an increasing concern for the protection of freedom of expression when the public interest is at stake.[68] Even in defamation law, which is not directly subject to Charter review, the Supreme Court of Canada took steps to make common law rules more consistent with freedom of expression.[69] In our view, and as further discussed below, a RTBF would infringe the constitutional right to freedom of expression of search providers, authors and webmasters, by hindering access to information.[70]

- **Search engine operators:** Search engines retrieve information from an immense pool of data, organizing and ranking such information by displaying results. In our view, there is little doubt that the Charter protects these results as matters of "expression". Indeed, the Supreme Court of Canada has already stated that hyperlinks "communicate that something exists".[71] Such an activity undeniably conveys "meaning" that falls within the scope of section 2(b).[72]

  We cannot overstate the importance of search engine results with respect to the exercise of freedom of expression in today's world. It is worth citing the Supreme Court of Canada about the essential role of hyperlinks:[73]

---

[65] *Torstar*, *supra* note 42, at para. 1 and 47; *Irwin Toy Ltd*., *supra* note 37, at 976; *Montréal (City)* v. *2952-1366 Québec Inc*., 2005 SCC 62, at para. 74.

[66] *Torstar*, *supra* note 42, at para. 105-06; referring to the defence of "fair comment" in defamation law. For a discussion of the notion of "public interest" under Canadian case law, see section 2.2.2 of this papier.

[67] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 43-13.

[68] *Bou Malhab* v. *Diffusion Métromédia CMR inc*., 2011 SCC 9, at para. 20-21 and 25.

[69] With respect to defamation law, the Supreme Court of Canada recently reinforced the defence of fair comment and created a new defence for responsible communication on matters of public interest, which applies, regardless of the truth of a statement, when the defendants can prove that they acted responsibly in gathering and publishing information. Interestingly, this defence is offered not only to journalists but to anyone who publishes material on any medium, including "new ways of communicating" such as blogs and – presumably – social media. *Torstar*, *supra* note 42, at para. 65, 85 and 96; *WIC Radio Ltd.* v. *Simpson*, 2008 SCC 40, at para. 28; It should be noted that the civil law province of Quebec has different rules in regard to defamation. See e.g. *Gilles E. Néron Communication Marketing Inc*. v. *Chambre des notaires du Québec*, 2004 SCC 53, at para. 56. See also section 2.2.1 of this paper, which discusses this relevant legal framework.

[70] With respect to the many persons – search providers, authors, webmasters, Internet users – whose freedom of expression might be infringed by the RTBF, see Edward Lee, "*The Right to Be Forgotten vs. Free Speech*", (2015) *I/S:* A Journal of Law and Policy for the Information Society [forthcoming], at 7-8 [Lee, "*The Right to Be Forgotten vs. Free Speech*"].

[71] *Ibid*, at para. 30.

[72] As a matter of comparison, a few U.S. District Courts have come to the conclusion that search results are protected under the First Amendment. See e.g. *Zhang* v. *Baidu.com, Inc*., 932 F.Supp.2d 561, at 11 [*Baidu.com*].

[73] *Crookes* v. *Newton*, 2011 SCC 47 [*Crookes*]; citing *Society of Composers, Authors and Music Publishers of Canada* v. *Canadian Assn. of Internet Providers*, 2004 SCC 45, at para. 40. The Court refers to the publication rule of defamation law which makes

> [34] The Internet's capacity to disseminate information has been described by this Court as "one of the great innovations of the information age" whose "use should be facilitated rather than discouraged" […]. Hyperlinks, in particular, are an indispensable part of its operation. [...]
>
> [36] The Internet cannot, in short, provide access to information without hyperlinks. Limiting their usefulness by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression. The potential "chill" in how the Internet functions could be devastating, since primary article authors would unlikely want to risk liability for linking to another article over whose changeable content they have no control. Given the core significance of the role of hyperlinking to the Internet, we risk impairing its whole functioning. Strict application of the publication rule in these circumstances would be like trying to fit a square archaic peg into the hexagonal hole of modernity. [References omitted]

In light of the above comments, there is little doubt that search engine results are expression within the meaning of section 2(b) of the Charter and would therefore benefit from its protection. As such, a RTBF would violate search engine operators' fundamental right to freedom of expression and would need to be justified under section 1 of the Charter.

- **Authors:** Freedom of expression entails the right to say nothing or the right not to say certain things.[74] Accordingly, search engine operators have the right not to display certain information. In fact, Google voluntarily delists highly sensitive information, such as signatures and bank accounts, and de-ranks web pages which repeatedly infringe copyrights.[75] Since the Charter does not apply directly to private corporations, we believe that authors could hardly challenge on constitutional grounds such decisions made by search engines.[76] However, the authors' constitutional right to freedom of expression would likely be violated if a statutory RTBF was to prevent search engines from displaying results pointing toward their works. Indexation on search engines has become invaluable for anyone wishing to disseminate information. It follows that any legal interference with search engine results would impact the freedom of expression of authors publishing online.[77]

---

publishers liable for the defamatory content they circulate. In *Crookes*, the Supreme Court of Canada stated that publishers of hyperlinks should not be liable for the defamatory content to which they refer, unless the link itself is defamatory. See also section 2.3.1 of this paper which discusses laws regulating intermediaries.

[74] *RJR-MacDonald Inc*. v. *Canada (Attorney General)*, [1995] 3 SCR 199, at para. 113 and 124. As a matter of comparison, see *Baidu.com*, *supra* note 72, at 5-7 and 16, where the U.S. District Court for the Southern District of New York held that the Chinese search engine Baidu can block, under the First Amendment, information pertaining to the "democracy movement in China" from its search results displayed in the U.S.

[75] Lee, "*The Right to Be Forgotten vs. Free Speech*", *supra* note 70.

[76] The voluntary removal of information by search engines might still lead to private litigation. In Quebec, for instance, it should be noted that the Quebec Charter does apply to private corporations. Under certain circumstances, the delisting of content might be considered as an abuse of right or as discriminatory conduct.

[77] About the legitimate expectation of authors that their works be disseminated via search engines, see e.g. Gianluigi Marino, "Right to be forgotten and the Google Advisory Council in Rome: main takeaways" (9 November 2014), online: Privacy Matters - DLA Piper <http://blogs.dlapiper.com/privacymatters/right-to-be-forgotten-and-the-google-advisory-council-in-rome-main-takeaways/>.

- **Webmasters:** Webmasters play a key role in disseminating the works of the authors and they equally have an interest in having the public access their webpages freely. In all likelihood, a RTBF could constitute a violation of their freedom of expression.

- **The public's right to access to information:** At this point, it seems hard to determine with any certainty whether a member of the public could directly challenge a RTBF by claiming a right to access to information. In *National Post,*[78] the Supreme Court of Canada recognized that freedom of expression protects readers and listeners, as well as writers and speakers, and that freedom of expression involves a freedom to gather information.[79] However, in *Globe and Mail,*[80] the Court rejected the notion of a fundamental right to access to information. In light of this latter decision, we believe it would be far-fetched to interpret the right to freedom of expression so as to include a constitutional right to access information through search engines. In any event, the fact that the public is deprived of access to certain information would no doubt be considered by Canadian courts when assessing the justification of any violation of the freedom of expression of search engine operators, authors and webmasters.

While a RTBF would not erase *per se* the original source of information, it would directly seek to hide information, by removing results for queries that include certain names. As such, we are of the view that a RTBF would breach the constitutional right to freedom of expression of search engine operators, authors and webmasters.

1.3 Can the RTBF be a justified limit to freedom of expression?

Now that we have established that a RTBF would, in all likelihood, infringe the right to freedom of expression, we will proceed with the justification test to determine whether such infringement could be deemed constitutional. Before going further, it is important to reiterate that limitations to Charter rights can only be justified under section 1 of the Charter if they are "prescribed by law", that is, if they are incorporated in a statute, a regulation or any other enactment of general application. Accordingly, we assume that the RTBF would be included in a statute.

The analysis under section 1 of the Charter is highly influenced by the language of the impugned provisions and the context of the case. Therefore, the constitutional validity of a RTBF would necessarily depend on how it would be implemented by the legislator and how far it would go in violating freedom of expression. For our purposes, we will analyze the RTBF as including the following features, as adopted in *Google Spain*:[81]

- The RTBF is the right to obtain from a search engine the erasure, from the list of results displayed following a search made on the basis of a person's name, of links to web

[78] *R.* v. *National Post*, 2010 SCC 16, at para. 28 [*National Post*]. See also *Edmonton Journal* v. *Alberta (Attorney General)*, [1989] 2 SCR 1326, at 1339-40 [*Edmonton Journal*]; and *Ford*, *supra* note 59, at 767.

[79] *National Post*, *supra* note 78, at 33 and 40.

[80] *Globe and Mail* v. *Canada (Attorney General)*, 2010 SCC 41, at para. 34 [*Globe and Mail*], where the Supreme Court of Canada found that s. 44 of the Quebec Charter, which expressly protects access to information "to the extent provided by the law", does not confer a "fundamental right" to information.

[81] *Google Spain SL*, *supra* note 3, at 88-99. See also Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González'* C-131/12" (26 November 2014), at 7-10.

pages published by third parties and containing certain information relating to that person (i.e. delisting or deindexing);

- The right would apply when the information appears, in light of all the circumstances, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the search engine operator; even when the information in question is true and its publication is lawful;
- The claimant does not have to show that the information causes prejudice;
- When personal information appears to be "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue", there is a rebuttable presumption to the effect that the RTBF overrides the interests of the search engines and of the general public;
- The aforementioned presumption may be rebutted, in specific cases, depending on the nature of the information in question and its sensitivity to the individual's private life and the interest of the public in having that information. As such, the role played by the claimant in public life can be taken into account;
- Search engine operators need to apply the above rules on a case-by-case basis;
- If the request is denied, the claimant can apply to privacy authorities or to the courts to reverse the decision. On the other hand, third parties cannot challenge the decision when the request is granted.

The requirement that the limitations be "prescribed by law" entails that the law provides sufficiently clear standards to avoid arbitrary applications. If it does not, the limitations will be held to be void. With respect to the RTBF, it could be argued that the criteria set out in *Google Spain* fail to offer such an intelligible standard. However, the courts are generally reluctant to strike down legislation on such basis, even when limits are couched in vague terms,[82] and we will therefore work on the premise that the RTBF would pass this preliminary test.

At this point, we will examine each step of the *Oakes*[83] test to determine whether legislation providing for a RTBF may justify a limitation of the freedom of expression. Throughout our analysis, we should keep in mind that the Supreme Court of Canada has recognized that hyperlinks – and, presumably, search results – have become essential tools to disseminate, find and access information.[84] As such, they can easily be said to support, in a myriad of ways, the core values of freedom of expression, namely democratic discourse, truth-finding and self-fulfilment.

The Supreme Court of Canada has stressed, in *Edmonton Journal,*[85] how important freedom of expression is to a democratic society, adding that it is only in very limited circumstances that this right can be restricted:

---

[82] See Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-16-18. For a rare example of a law found to be void for vagueness, see *Crouch* v. *Snell*, 2015 NSSC 340, at para. 130 [*Crouch*], where the Nova Scotia Supreme Court struck down a provincial anti-cyberbullying act, which was held to provide no standard so as to avoid arbitrary decision-making; This case is further discussed in section 2.2.2.

[83] *Oakes*, *supra* note 34, at 135-140.

[84] *Crookes*, *supra* note 73, at para. 34-36.

[85] *Edmonton Journal*, *supra* note 78, at 1336.

> It is difficult to imagine a guaranteed right more important to a democratic society than freedom of expression. Indeed a democracy cannot exist without that freedom to express new ideas and to put forward opinions about the functioning of public institutions. The concept of free and uninhibited speech permeates all truly democratic societies and institutions. The vital importance of the concept cannot be over-emphasized. No doubt that was the reason why the framers of the Charter set forth s. 2(b) in absolute terms which distinguishes it, for example, from s. 8 of the Charter which guarantees the qualified right to be secure from unreasonable search. It seems that the rights enshrined in s. 2(b) should therefore only be restricted in the clearest of circumstances.

These comments entail the consequence that any limitation on freedom of expression would need to satisfy a stringent justification test.

1.3.1 Pressing and substantial objective

The first step requires assessing whether the objective of the infringing measure is sufficiently important to justify overriding freedom of expression. In practice, this requirement has been met in nearly all decisions rendered by the Supreme Court of Canada. Clearly, the latter tends to avoid questioning the virtues of the legislators' objectives. As such, the burden of proof is rather easy to satisfy in this regard.[86]

The RTBF would be an answer to the Internet's almost unlimited capacity to remember, which can make the "worst moments of our lives" – as well as utterly false allegations – readily available forever.[87] In *Google Spain,*[88] the Court of Justice of the European Union has further pointed out that search engines give Internet users an unprecedented capacity to obtain the profile of a given individual, generating new risks for privacy. In other words, privacy is no longer protected by the mere difficulty of remembering or finding information,[89] as would be the case with the hard copy of a newspaper published years ago.

The Supreme Court of Canada has already acknowledged this problem. In *UFCW,*[90] a leading case on freedom of expression and privacy, the Court has highlighted that data protection laws seek to avoid the "potential harm that flows from the permanent storage or unlimited dissemination of personal information through the Internet".

The objective of a RTBF could be described as providing an individual with some measure of control over personal information that is disseminated on the Internet and that creates a risk of harm.[91] Such an

---

[86] See Hogg, *Constitutional Law of Canada*, *supra* note 21, 38-22-23.

[87] See Michael Douglas, "Questioning the Right to Be Forgotten" (2015) 40:2 Alt J 109, at 109 and 112.

[88] *Google Spain SL*, *supra* note 3, at para. 80.

[89] See Patricia Kosseim, "The (in)finite life of personal information in a digital age" (Address delivered at the Yukon Bench and Bar Seminar, 10 September 2015), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/media/sp-d/2015/sp-d_20150910_pk_e.asp>.

[90] *UFCW*, *supra* note 32, at para. 23.

[91] On the notion that data protection laws should aim at protecting information that can create a risk of harm to individuals, see Gratton, *Understanding Personal Information: Understanding Privacy Risks*, *supra* note 16, at 201-202. With regard to the purpose of the RTBF, see also Policy and Research Group of the Office of the Privacy Commissioner of Canada, "Online Reputation, What are they saying about me?", *supra* note 15, at 5.

objective is connected to fundamental values, such as privacy, dignity and autonomy.[92] In all likelihood, this objective would be recognized as sufficiently important to justify a limit on freedom of expression.

1.3.2 Rational connection between the law and its objective

This requirement is aimed at preventing arbitrary limitations. At this stage of the analysis, the government (or any party seeking to uphold the law) must show a rational connection between the infringement and the benefits sought. Logic and reason are sufficient to make this demonstration. At this stage, there is no need to prove the efficiency of the impugned law.[93] Again, the threshold is not difficult to meet and there are very few cases where a law has been nullified on that ground.[94]

With respect to the RTBF, the ability to request the delisting of certain links from search results is undeniably connected to the objective of empowering individuals, so that they can better control the dissemination of their personal information on the web. The rational connection requirement would therefore not, in our view, be the subject of extensive debate.

1.3.3 Minimum Impairment

The third step is usually the most difficult to satisfy. It requires showing that the law impairs the right in question "no more than necessary to accomplish the desired objective".[95] In other words, the question is whether the same goal could possibly be achieved in a significantly less infringing manner.[96] The legislator is, however, given some leeway. To the extent that the law falls within a range of reasonable, least drastic alternatives, it will pass the test, even though the objective could be accomplished in a slightly less infringing manner.[97]

Despite the leeway given to the legislator, however, we believe that the RTBF, as defined above, would likely fail the test of minimum impairment.

The criteria set out by *Google Spain* – that the information appears "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue […]"[98] – are in our view far too broad and subjective and would necessarily result in delisting information of public interest beyond the objective sought by the legislator:

---

[92] *UFCW*, *supra* note 32, at para. 19.

[93] *Hutterian Brethren of Wilson Colony* v. *Alberta*, 2009 SCC 37, at 48 [*Hutterian Brethren of Wilson Colony*].

[94] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-34.1. For a noteworthy exception where the Supreme Court of Canada declared a limitation to freedom of expression invalid for lack of rational connection, see *Whatcott*, *supra* note 61, at para. 92. In this ruling on anti-hate speech provisions, the Court found that the words "ridicules, belittles or otherwise affronts the dignity of" were not rationally connected to the legislative purpose of addressing systemic discrimination.

[95] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-36.

[96] *Hutterian Brethren of Wilson Colony*, *supra* note 93, at para. 66. See also *Carter* v. *Canada (Attorney General)*, 2015 SCC 5, at para. 102.

[97] *Hutterian Brethren of Wilson Colony*, *supra* note 93, at para. 53-55.

[98] For our purposes, we will not take into account the non-binding Guidelines on the implementation of the *Google Spain* decision proposed by the Article 29 Data Protection Working Party of the European Union. See Article 29 Data Protection Working Party, "*Guidelines on the Implementation of the Court of Justice of the European Union Judgment*" on "*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González*" C-131/12", *supra* note 81.

- **Inadequate** – What is "adequate" for one might not be for another. Apart from content such as child pornography, "revenge porn" and Magnotta-like videos, there is probably little consensus as to what is "inadequate" information on the Internet. One might also wonder to what extent alleged inaccuracies make the information "inadequate".[99] The accuracy of the information might be difficult to verify, as is often the case in matters of defamation. Is the search provider expected to conduct some kind of investigation? If not, should the claimant's allegations be taken at face value? Pursuant to such criteria, it seems that a mere appearance of "inadequacy" – whatever that means – might be enough to hinder access to content of an inherently public interest character.

- **Irrelevant** – Nothing is more subjective than relevance. To whom is the information supposed to be relevant? In what respect? What is "relevant" for one might not be for another. It may vary greatly depending on the context or across jurisdictions.

- **No longer relevant** – When does information lose relevance? After 5, 10, 15 years? What if the deindexed information later regains relevance due to changes in circumstances, as might be the case if an individual who had cleansed the search results linked to his name later ran for election?[100]

- **Excessive in relation to the purposes of the processing at issue** – This criterion appears to be difficult to apply to search engines, as opposed to other data controllers which generally collect information for the purpose of conducting their business. Here, the "processing at issue" presumably refers to the displaying of search results. How can it be "excessive" in regard to its purpose, which is to make the information readily available?

- **Role played in public life** – The search provider must also take into consideration the role played by the claimant in public life. What is the scope of "public life"? Is it mostly limited to politicians and elected officials? Does it extend to public servants, business people, professionals and/or journalists? Are well-known artists and athletes necessarily involved in "public life"? Should local, national and international public figures be treated on an equal basis? Is the search provider expected to conduct research to determine whether the claimant plays a role in public life? Otherwise, how should it be assessed?

Such criteria confer almost unfettered discretion in dealing with removal requests and, as a result, with the freedom of expression of third parties.

Canadian courts have struck down legislation when confronted with vague and subjective standards. For instance, with regard to the false-news offence of the *Criminal Code*[101] of Canada, which prohibited deliberately false statements likely to cause "injury or mischief to a public interest", the Supreme Court of Canada reached the conclusion that the provision was so vague that it infringed freedom of

[99] In matters of personal information, accuracy and adequacy are considered to be closely related. See Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González'* C-131/12", *supra* note 81, at 15.

[100] See Patricia Sánchez Abril & Jacqueline D. Lipton, "The Right to Be Forgotten: Who Decides What the World Forgets" (2014-15) 103 Ky LJ 363, at 383 [Sánchez Abril & Lipton].

[101] RSC 1985, c. C-46.

expression more than necessary to secure the legislation's objectives.[102] Recently, the Nova Scotia Supreme Court held that an anti-cyberbullying act failed to define cyberbullying so as to avoid overbreadth.[103]

In the matter at hand, the vagueness of the criteria is compounded by the fact that the RTBF would be enforced by private corporations. As many commentators have pointed out, these corporations have an incentive to err on the side of removal[104] to reduce costs and/or to avoid legal liability and the hefty fines to which they are exposed in case of non-compliance.[105] This should give us pause as to the reasonableness of entrusting private entities with the tasks of arbitrating fundamental rights and values and determining what is in the public interest, with little or no government or judicial oversight.[106] Without transparency and openness, nothing guarantees the integrity of the process.[107]

In addition, the process adopted in *Google Spain* appears to be biased in favour of the claimant, thus increasing the likelihood that information of public interest being removed from search results. Authors, webmasters and members of the public are not notified of a complaint and have no way to intervene and demonstrate that the information is adequate and relevant. In fact, search engines have no obligation to alert page owners of the delisting.[108] Moreover, while claimants can resort to privacy authorities and to the courts if dissatisfied with the decision, nobody else can challenge it.[109] This one-sided approach is a blatant breach of the most basic principles of procedural fairness, and Canadian courts would most likely consider this aspect if and when called upon to determine whether or not the RTBF could be justified under section 1 of the Charter.[110]

---

[102] *Zundel*, *supra* note 60, at 768-775.

[103] *Crouch*, *supra* note 82, at para. 165.

[104] As of March 2016, Google has granted 42% of about 400,000 removal requests it received in Europe. See Google, "Transparency Report: European Privacy Requests for Search Removals", *supra* note 11.

[105] European authorities may impose fines for non-compliance with privacy legislation. See e.g. Cunningham, "The Internationalization of Censorship", *supra* note 8, at 24; Douglas, "Questioning the Right to Be Forgotten", *supra* note 87, at 110 Sánchez Abril & Lipton, *supra* note 100, at 382-385; This issue is further discussed in section 2.3.1 of this paper.

[106] Sánchez Abril & Lipton, *supra* note 100, at 366.

[107] It should be noted that the Supreme Court of Canada has recognized the importance of openness for the proper administration of justice. See e.g. *Canadian Broadcasting Corp*. v. *Canada (Attorney General)*, 2011 SCC 2, at para. 29. Similarly, in light of the fundamental values at stake, we believe that some level of transparency would be necessary in implementing the RTBF.

[108] Google has nevertheless decided to notify webmasters that a link has been removed. See Cunningham, "The Internationalization of Censorship", *supra* note 8, at 27. See also Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González'* C-131/12", *supra* note 81, at 10.

[109] See Leonid Sirota, "*The Power of Google, Squared*" (16 March 2015), online: Double Aspect <https://doubleaspectblog.wordpress.com/2015/03/16/the-power-of-google-squared/>; citing Andrew McLaughlin, former CEO of Digg and former Director of Public Policy for Google. See also Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González'* C-131/12", *supra* note 81, at 7.

[110] As a matter of comparison, the Supreme Court of Canada has stressed that a court should give the media an opportunity to be heard before issuing a publication ban. See e.g. *Globe and Mail*, *supra* note 80, at para. 74-75. We believe that the same logic should apply, to some extent, to the removal of links pointing toward authors' works.

The bias is further aggravated by the creation of a presumption that the RTBF trumps, as a general rule, the interest of the public in accessing the information in question, upon the demonstration that the personal information appears to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue. Although the interest of the public may in principle override the claimant's rights, how can the presumption be rebutted if those whose rights are at stake are prevented from intervening and making representations to the decision-maker? As it currently stands, the burden rests on the "arbitrator" itself, that is, the search engine operator. In our view, the presumption should rather play in favour of freedom of expression, as this approach would be more consistent with Canadian case law.

For instance, in *Edmonton Journal,*[111] the Supreme Court of Canada struck down provisions which restricted to a minimum the publication of information related to matrimonial proceedings. While recognizing the importance of protecting privacy, the Court gave more weight to the public's interest in being informed. In *Torstar,*[112] while balancing the values underlying the freedom of expression against the right to reputation, the Court gave priority to the former in broadening the defences against defamation.

Finally, it should be remembered that an individual using his or her RTBF has no obligation to demonstrate any prejudice or even a mere risk of harm.[113] In our view, the claimant should have the burden of showing that the dissemination of his/her personal information definitely causes a certain harm or, at the very least, a risk of harm; otherwise the public interest to be informed should prevail over any such purely private interest. Under certain circumstances, such a requirement might help prevent the removal of information relevant to the public. For instance, if an individual requested the delisting of certain information with a view to running in an election for public office, it might be more difficult for him or her to hide his or her true intentions if a risk of harm actually had to be demonstrated.

As proposed, the RTBF could hardly be considered one of the least drastic means to achieve the desired goals, as it lacks proper limitations. Information that need not be protected would get caught in the net, restricting unnecessarily search engines' ability to display results and authors' ability to disseminate information. It remains true that the information in question would still be available online, and that it would only be deindexed from queries on certain names. By preventing search by name, however, the RTBF would make certain information of interest much more difficult, if not totally impossible, to find, thus hindering the free flow of information.

At this point, it suffices to say that there are certainly more tailored alternatives than the one proposed in *Google Spain* that would accomplish the same objectives, without infringing more than necessary Canadians' freedom of expression.

---

[111] *Edmonton Journal*, *supra* note 78, at 1346-1350.

[112] *Torstar*, *supra* note 42, at para. 65. Since the Charter does not apply directly to defamation law in common law jurisdictions, this case did not involve the justification test of section 1.

[113] In Europe, the non-binding Article 29 Data Protection Working Party Guidelines do suggest to consider "harm" as a factor in balancing the claimant's right to privacy and the interest of the public, though it is not considered a condition for exercising the RTBF. See also Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on '*Google Spain and inc v. Agencia Española de Protección de Datos (AEPED) and Mario Costeja González'* C-131/12", *supra* note 81, at 18.

1.3.4 Proportional Effect

The fourth and final step of the analysis is to determine whether the deleterious effects of the infringement are proportionate to their benefits.[114] Given our conclusion that the RTBF is not minimally impairing, it would not be necessary to examine this requirement. However, for our purposes, we will proceed with the analysis, assuming a RTBF would satisfy the first three criteria.

Proportional effect is rarely an issue when the first three criteria are met.[115] Nevertheless, we believe that a RTBF would fail this last test, especially in light of comments made by the Supreme Court of Canada in *UFCW,*[116] one of the few cases where a law was struck down on that ground. In *UFCW*, the question was whether Alberta's *Personal Information Protection Act* ("PIPA") could prevent a union from video-taping and photographing individuals crossing the picket-line during a strike. As is the case with the RTBF, the statute protected *all* information about an identifiable individual.

The Supreme Court of Canada gave little weight to the benefits of the law in terms of privacy. The Court observed that the statute's definition of "personal information" was over-inclusive. Such a definition implied that any information related to an individual was protected, regardless of its context, even if no intimate details were revealed.[117] Under these circumstances, the Court gave priority to the union's freedom of expression and declared the entire statute invalid.[118]

Similarly, a RTBF would extend to "personal information" which is not intrinsically private, including information pertaining to the claimant's public activities. The benefits of protecting such information are of limited value. It should be noted that, in matters of state intrusion, constitutional protection of privacy does not extend to the all-encompassing category of "personal information" as defined in personal protection statutes.[119] It is restricted to a "biographical core of information", which includes "intimate personal details".[120] Moreover, an individual is only entitled to a "reasonable expectation of privacy" which may vary depending on the context.[121] Even under the Quebec Charter, which expressly guarantees the right to privacy, the purpose of the protection is to allow for a "sphere of personal

[114] *Hutterian Brethren of Wilson Colony*, *supra* note 93, at para. 72-76.

[115] Hogg, *Constitutional Law of Canada*, *supra* note 21, at 38-43-44.

[116] *UFCW*, *supra* note 32. The *UFCW* decision is further discussed in section 2.1.1 of this paper.

[117] *Ibid*, at para. 25-26.

[118] *Ibid*, at para. 37-41. Alberta's *Personal Information Protection Act* ("PIPA") was declared invalid specifically because it imposed disproportionate restrictions to the union's ability to communicate with the public, in the context of a strike. However, the reasons for the judgment, especially the overbreadth of the definition of "personal information", call into question the very constitutionality of all Canadian data protection laws, since they all contain similar definitions of "personal information". With respect to the over-inclusiveness of the definition of "personal information", see Cunningham, "The Internationalization of Censorship", *supra* note 8, at 29-31; and Gratton, *Understanding Personal Information: Understanding Privacy Risks*, *supra* note 16, at 93-106.

[119] Power, *The Law of Privacy*, *supra* note 31, at 237-240.

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

[121] *Hunter*, *supra* note 31, at 159.

autonomy" in regards to "choices that are of a fundamentally private or inherently personal nature".[122] It does not protect every piece of data related to an identifiable individual.

In other words, we believe that a RTBF would cover information far remote from the value of privacy which underlies the Canadian Charter (and the Quebec Charter, for that matter). Conversely, search engine results contribute to the core purposes of the constitutional right to freedom of expression, namely democratic discourse, truth-seeking and self-fulfillment. They make research much easier and accessible to ordinary citizens and facilitate the dissemination of works and ideas. In that sense, search results can be said to be a democratizing force.[123] As such, they should only be restricted in the clearest of circumstances.

Moreover, the failure to consider the risk of harm entails the risk that some claimants might make requests based on mere whims. Yet, according to the Supreme Court of Canada, restricting expression simply because of "hurt feelings" does not give sufficient weight to the role that expression plays in our society.[124] As the Court put it, with respect to the right to reputation,[125] "freewheeling debate on matters of public interest is to be encouraged, and must not be thwarted by 'overly solicitous regard for personal reputation'".[126]

In our view, the benefits of delisting "personal information" that is not inherently private and that causes no harm cannot outweigh the deleterious effects on freedom of expression, especially considering that authors and webmasters will have no say as to the relevance and adequacy of the information in question. We therefore believe that a RTBF would fail to satisfy the last stage of the *Oakes* test, even assuming that the minimal impairment test is met. However, if the RTBF was tailored so as to apply exclusively to intrinsically intimate and significantly harmful information (the victims of "revenge porn" come to mind),[127] its benefits might justify such purposive limits on the freedom of expression.

***

In light of the foregoing, we believe that the RTBF, at least as defined in Europe, would likely infringe upon the right to freedom of expression in a way that cannot be demonstrably justified under section 1 of the Canadian Charter. Accordingly, any law purporting to create such a right might well be struck down. This conclusion also makes it unlikely that a Canadian court would construe existing statutes – or the common law, for that matter – so as to grant a right to request that certain personal information be

---

[122] *Aubry*, *supra* note 45, at para. 52-57, where the Supreme Court of Canada held that the public's right to information, supported by freedom of expression, places limits on the Quebec Charter's right to privacy. This case is further discussed in section 2.2.2 of this paper.

[123] Leonid Sirota, "The Power of Google" (21 September 2014), online: Double Aspect <https://doubleaspectblog.wordpress.com/2014/09/21/the-power-of-google/>.

[124] *Whatcott*, *supra* note 61, at para. 109, where the Supreme Court of Canada declared parts of Alberta's anti-hate speech provisions invalid.

[125] The Supreme Court of Canada has stated that the right to reputation is "intimately" related to privacy. *Torstar*, *supra* note 42, at para. 59.

[126] *Ibid*, at para. 52.

[127] In fact, Google has already taken steps to cope with the "revenge porn" phenomenon. See Lee, "*The Right to Be Forgotten vs. Free Speech*", *supra* note 70, at 19-22, where the author also suggests that protecting victims of traumatic crimes might be a justifiable purpose for a limited right to be forgotten.

deindexed from search results. When possible, courts will avoid an interpretation which would be inconsistent with the Constitution of Canada.

However, as mentioned above, a limited RTBF might possibly strike an appropriate balance between freedom of expression and privacy, if it was limited to intrinsically intimate information which creates a significant risk of harm. Moreover, such a policy might be much more justifiable if, instead of leaving its enforcement to search engines, legal mechanisms were set up to allow authors, publishers and members of the public to assert their rights.

2. CANADIAN LEGAL FRAMEWORK ADDRESSING RTBF CONCERNS

A RTBF is usually meant to address privacy and reputational concerns resulting from the fact that personal information is more easily available online than elsewhere and for longer periods of time. According to the OPC, individuals' ability to manage their reputation depends on their ability to control the availability of their personal information to others and the context in which it is accessed and used.[128] Before determining if we need a RTBF in Canada, we therefore first need to assess the legal framework already in place, determine whether this framework has proven adequate or sufficient to address individuals' privacy and reputation concerns, as well as to ascertain what are its limits.

This section will discuss the legal right for individuals to have information about themselves erased or deleted through applicable data protection laws, laws restricting the availability or use of certain types of information, laws restricting the dissemination of information or which can be used to protect one's privacy and reputation, as well as take-down laws and tools available in Canada.

2.1 Laws Allowing Individuals to Control their Personal Information

The current legal framework in Canada already allows individuals to control their personal information. Indeed, existing laws already include, at least to a certain extent, the principles underlying the RTBF. As will be shown in the two subsections below, these laws include data protection laws, such as PIPEDA and other substantially similar provincial statutes, but also enactments restricting the availability or the use of personal information, such as credit reporting legislation, amongst other laws.

2.1.1 Data Protection Laws and Right of Erasure

Data protection laws generally include a right allowing individuals to control their personal information, and they are usually the laws most readily associated with the RTBF. For instance, some have articulated the view that the right to be forgotten can more or less be reflected through the current obligations in data-protection legislation to delete personal data when no longer relevant or inaccurate, or following a justified objection by the data subject.[129] European Commissioner Viviane Reding refers to the RTBF as an element of the review of the Directive 95/46/EC, which envisions "strengthening the so-called 'right to be forgotten'",[130] which implies that this right already exists and is simply in need of reinforcement.[131]

In Canada, the private sector data protection regime includes the *Personal Information Protection and Electronic Documents Act*[132] ("PIPEDA"), which is the default statute, applying to the collection, use or disclosure of personal information by the private sector in the course of commercial activity.[133] In

[128] "Online Reputation, What are they saying about me?", *supra* note 15.

[129] Meg Leta Ambrose and Jef Ausloos, "The Right to Be Forgotten Across the Pond" (2012) 3 Journal of Information Policy 1, at 14. See also Directive 95/46/EC, *supra* note 1, art. 6(1)(e), 12(b) and 14.

[130] Viviane Reding, "The Upcoming Data Protection Reform for the European Union" (2011) 1 International Data Privacy Law 3, at 4.

[131] Bert Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice" (2011) 8-3 SCRIPTed 229, at 4-5.

[132] *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5 [PIPEDA].

[133] See s. 4(1)(a) of PIPEDA.

certain provinces, substantially similar provincial legislation[134] applies to the collection, use and disclosure of personal information in the private sector, with respect to activity taking place in an intra-provincial context: These are Alberta PIPA,[135] the British Columbia *Personal Information Protection Act*[136] (the "B.C. PIPA") and the Quebec *Act Respecting the Protection of Personal Information in the Private Sector*[137] (the "Quebec ARPPIPS"). Individuals who believe an organization covered by PIPEDA or one of these provincial statutes is not living up to its legal responsibilities have the right to file a complaint with the relevant regulator who will conduct an investigation.[138]

Data protection laws, such as PIPEDA and substantially similar provincial laws, already include, to a certain extent, the principle underpinning the right to be forgotten. Like Directive 95/46/EC, these laws already cater to a RTBF in Canada, through certain rights and principles such as the data collection limitation principle (prohibiting an organization from collecting more personal information than *necessary* for the purpose identified) as well as the data use, disclosure and retention limitation principle (precluding an organization from using or disclosing more personal information than *necessary* for the purpose identified). These laws also usually provide for a right for the individual to consent to his or her collection of personal information and to be able to withdraw such consent, a right to have personal information amended to ensure its accuracy, and a right to request that the information be deleted if it is no longer necessary.[139] That being said, these rights are not identical to the RTBF.[140] While the RTBF affects search engines, the right to erasure places responsibility on the organization that collects and processes the information in the first place (i.e. webmasters). Moreover, these laws have some limits in addressing privacy and reputational concerns, given that some information collectors may not necessarily post the information they collect in a commercial capacity and therefore, may not be subject to these laws. As a matter of fact, PIPEDA applies to an organization that collects, uses or discloses personal information in the course of commercial activities.[141] Provincial data protection laws have similar limitations.[142]

---

[134] The Quebec, Alberta and British Columbia private sector data protection statutes have all been found to be substantially similar. See *Organizations in the Province of Alberta Exemption Order*, S.O.R./2004-219; *Organizations in the Province of British Columbia Exemption Order*, S.O.R./2004-220; and *Organizations in the Province of Quebec Exemption Order*, S.O.R./2003-374.

[135] SA 2003, c. P-6.5 [Alberta PIPA].

[136] SBC 2003, c. 63 [B.C. PIPA].

[137] CQLR, c. P-39.1 [ARPPIPS].

[138] At the federal level, the Office of the Privacy Commissioner handles these complaints. Alberta and B.C. each has an Office of the Information and Privacy Commissioner and Quebec's complaints are handled by the Commission d'accès à l'information.

[139] It has been raised that, in practice, there is very little enforcement of this last rule, since organizations have a significant margin of appreciation in determining for how long retention of personal information still serves their purpose. Hans Graux, Jef Ausloos, Jef & Peggy Valcke, "The Right to Be Forgotten in the Internet Era" (2012) ICRI Research Paper No. 11, at 10.

[140] For example, the European Parliament has warned that*:* "[t]he right to be forgotten should not be confused with the right to erasure under the EU General Data Protection Regulation." European Parliament, *Proposed General Data Protection Regulation* (12 March 2014 version).

[141] PIPEDA, s. 2(1) and 4(1)(a). However, Scassa explains that if commercial advertising were associated with a blog or website, or if some other revenue generating scheme were in place, the activity would likely fall within the scope of PIPEDA. See Teresa Scassa, "Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets and Information Maps" (2010) 35 Queen's L.J. 733 at 742 [Scassa].

[142] See e.g. Alberta PIPA, s. 1(1)(i) and 4(3)a); s. 3(2) of the B.C. PIPA, the Quebec ARPPIPS applies to private sector activity by those "in the course of carrying on an enterprise within the meaning of article 1525 of the *Civil Code of Quebec*." This includes

Similar to Directive 95/46/EC, which allows EU Member States to enact journalism exceptions, so long as they are "necessary to reconcile the right to privacy with the rules governing freedom of expression"[143] PIPEDA and the three provincial data protection laws from Alberta, B.C. and Quebec each contain similar exceptions for the collection, use or disclosure of personal information for journalistic purposes.[144] That being said, none of those laws define what "journalistic purposes" actually means.[145] Other jurisdictions with similar data protection statutes have also raised similar issues.[146] According to some authors, this leaves data published by bloggers, tweeters and other non-traditional media in a more vulnerable position.[147]

This journalistic purposes exception has been included in private sector data protection legislation to balance the public interest in protecting individual privacy with the public interest in freedom of expression as enshrined in section 2(b) of the *Charter*, a subject further discussed in section 1 of this paper. There has been relatively little case law interpreting the journalistic purposes exceptions under PIPEDA or equivalent provincial data protection enactments.[148]

Notwithstanding the constitutional challenges already discussed above, while Canadian data protection laws could, to a certain extent, play the role of legitimizing a RTBF in Canada, in the same way as Directive 95/46/EC and the related Data Regulation have in Europe, some authors have argued that the expansive definition of "personal information" dilutes its effect and undermines its main objective.[149] These authors argue that instead of having data protection laws that declare all personal information to be protected and that require organizations to delete personal information deemed "irrelevant," these laws should instead target specific harms that attend specific privacy violations.[150] If data protection laws, by capturing the processing of *all personal information*, are overreaching in their scope, a RTBF, if

---

individuals who provide a "service," "whether or not it is commercial in nature". See also *Conseil de presse du Québec c. Cour du Québec*, [2004] C.A.I. 649 (C.S.).

[143] Directive 95/46/EC, *supra* note 1.

[144] See PIPEDA, s. 4(2)(c); s. 4(3)(b) and 4(3)(c) of the Alberta PIPA; s. 3(2)(b) of the B.C. PIPA, Quebec ARPPIPS, s. 1.

[145] Scassa, *supra* note 141 at 745.

[146] See article 80 of the European Regulation which, similarly, requires that Member States provide an exemption for "journalistic purposes," but does not define "journalist". See art. 80 of General Data Regulation, *supra* note 2.

[147] See Cunningham, "The Internationalization of Censorship", *supra* note 8 at 29, discussing Michael L. Rustad & Sanna Kulevska, "Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow" (2015) 28 Harv. J.L. & Tech. 349 at 375-76; Patricia Sanchez Abril & Jacqueline D. Lipton, "The Right to be Forgotten: Who Decides What the World Forgets" (2014) 103 KY.L.J. 363 at 382 (asking whether information "published in a formal news media outlet" would be "treated differently from that published in a personal blog, social media website, or chat group").

[148] *Calgary Herald Group Inc.* (16 February 2007), OIPC Alberta Order P2005-004, [*Calgary Herald*]; *Alberta Bill of Rights*, R.S.A. 2000, c. A-14; *UFCW*, *supra* note 32; *Alberta Teachers' Association* (13 March 2008), OIPC Alberta Order P2007-014; *Chandra v. CBC*, 2015 ONSC 5303 at para. 59 and following; *Romana v. The Canadian Broadcasting Corporation et al*, 2016 MBQB 33 at para. 21 and following. Under the Quebec ARPPIPS, the exception for journalistic purposes uses wording that is similar to the wording used in relation to liability for invasion of privacy. A combination of *Civil Code* provisions and provisions in the Quebec *Charter of Human Rights and Freedoms* gives recourse in damages for those who believe their privacy rights have been invaded. These recourses are further discussed in section 2.2 below.

[149] See Gratton, *Understanding Personal Information: Understanding Privacy Risks*, *supra* note 16, at sections 2.1.1 "Privacy as an Absolute Right" and 2.1.2.1.1 "Potentially Over-inclusive Definition"; See also Cunningham, "The Internationalization of Censorship", *supra* note 8 at 30-31 and 35.

[150] *Ibid*. See also Eloïse Gratton, "If Personal Information is Privacy's Gatekeeper, then Risk of Harm is the Key: A proposed method for determining what counts as personal information" (2013) 24 Alb. L.J. Sci. & Tech. 105.

such right was ever recognized in Canada, could also be considered as being flawed in its application, due to the over-inclusiveness of any such statutes. It should be remembered that in a recent judgment rendered in a labour relations context, *Re United Food and Commercial Workers Local 401*,[151] the Supreme Court of Canada determined that the Alberta PIPA infringed the constitutional right to freedom of expression under the *Canadian Charter of Rights and Freedoms*. More importantly, the Court suggested that the all-encompassing scope of protection stipulated by the Alberta PIPA was overbroad and should be subject to limitations.[152] Since all Canadian data protection laws have a similar scope, constitutional challenges remain on the rise.[153]

2.1.2 Laws Restricting the Availability or Use of Information

Pasquale warns that "we could soon be in a world where each person one encounters can be instantly categorized as friend or threat, competent or pathetic, by software. To declare such technologies of reputation beyond the bounds of regulation is to consign myriad innocent individuals to stigma, unfairly denied opportunities, and worse."[154]

For Koops, there are two approaches in the literature that put forgetfulness in a slightly different perspective. The first emphasises the link with the "clean slate" or "fresh start" that has long been an element of several areas of law fostering social forgetfulness, such as bankruptcy law, juvenile criminal law, and credit reporting."[155] The second alternative approach mirrors the first, in that it looks at the "clean slate", not from the perspective of society but from the perspective of the individual.[156] Koops also explains how the RTBF as a control on a clean slate has a much more modest and narrower impact than the right to delete that currently dominates the debate, as it does not focus on comprehensive measures aimed at individuals being able to control what information exists, "but rather on fine-grained, context-specific measures aimed at controlling how other parties can use information when decisions are made that affect individuals."[157]

The OPC, in its recent Online Reputation Research Paper, discusses how "[a]nother proposed solution for mitigating harm from online information involves disallowing decision-making on the basis of online information, as long as this does not harm other members of society".[158] They quote, by way of example, several U.S. states which have recently enacted laws prohibiting prospective employers from

[151] *UFCW*, *supra* note 32.

[152] The significance of this court decision is potentially far-reaching since the Alberta PIPA is almost identical to the B.C. PIPA and is similar in many aspects to PIPEDA and the Quebec ARPPIPS. Therefore, the Court's indicated limitation on the permissible scope of data protection laws – that they may not infringe the constitutional right to freedom of expression – is likely to be relevant for those laws as well.

[153] This issue is further discussed in section 1.3.4 discussing the "Proportional Effect".

[154] Pasquale, *supra* note 10, at 537.

[155] Bert Jaap Koops, "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice" (2011) 8 SCRIPTed 229 at 5.

[156] *Ibid*.

[157] *Ibid*, at p. 24.

[158] "Online Reputation, What are they saying about me?", *supra* note 15, at 9.

requiring candidates to provide their social media passwords,[159] and discuss provincial authorities such as the *Ontario Human Rights Commission*[160] and the *British Columbia Office of the Information and Privacy Commissioner*,[161] both of which have issued guidelines to employers using social media for background checks, advising that such practices may put them in violation of applicable provincial statutes.

Several laws are already in force, in both the United States and Canada, to ensure that certain types of information will not be available after a certain period of time, or that it will not be used in making decisions that may affect individuals. These laws usually pertain to bankruptcy and credit, as well as criminal backgrounds.

- **Clean Slates and Criminal and Credit Information**

In the United States, the Federal Credit Reporting Act ("FCRA") requires that bankruptcies be removed from consumers' credit reports one decade after they occur.[162] Given the devastating impact a bankruptcy can have on an individual's reputation and credit history, this element of the FCRA was a particularly important advance in giving individuals a fresh start, as explained by Pasquale:

> [It] is not much good for an ex-convict to expunge his juvenile record, if the fact of his conviction is the top Google result for searches on his name for the rest of his life. Nor is the removal of a bankruptcy judgment from a credit report of much use to an individual if it influences lead generators' or social networks' assessments of creditworthiness, and would-be lenders are in some way privy to those or similar reputational reports.[163]

A similar type of legislation also exists in Canada. For example, with respect to bankruptcy and credit, most Canadian provinces have credit reporting legislation[164] that prevents consumer reporting agencies from including, in a credit report, information as to judgments or as to the bankruptcy of a consumer 6 or 7 years after a bankruptcy was rendered or from the date of the discharge.[165] With respect to criminal records, the *Criminal Records Act*[166] provides that a person who has been convicted of an offence under

---

[159] See for instance the U.S. States of Montana and Connecticut. National Conference of State Legislatures, "Access to Social Media Accounts and Passwords" (September 14, 2015), online: NCSL <http://www.ncsl.org/research/telecommunications-and-informationtechnology/employer-access-to-social-media-passwords-2013.aspx>.

[160] Ontario Human Right Commission Facebook page post dated March 23, 2012, online: OHRC <https://www.facebook.com/the.ohrc/posts/320570581329371>.

[161] Office of the Information and Privacy Commissioner of British Columbia, "Guidelines for Social Media Background Check" (October 2011), online: OIPCBC <https://www.oipc.bc.ca/guidance-documents/1454>.

[162] 15 U.S.C. § 1681c(a)(1) (2012):`"[N]o consumer reporting agency may make any consumer report containing . . . [bankruptcies that] antedate the report by more than 10 years.".

[163] Astra Taylor & Jathan Sadowski, "How Companies Turn Your Facebook Activity Into a Credit Score", *The Nation* (27 May 27 2015), online: The Nation <http://www.thenation.com/article/how-companies-turn-your-facebook-activity-credit-score/> discussed in Pasquale, *supra* note 10 at p. 516.

[164] Currently, New Brunswick, the Northwest Territories, Yukon and Nunavut do not have such legislation.

[165] See, paragraphs 109(1)f) and 109(1)g) of the British Columbia *Business Practices and Consumer Protection Act*, SBC 2004, c 2. The Ontario *Consumer Reporting Act* contains similar provisions, albeit with a 7-year (rather than a 6-year) rule. See *Consumer Reporting Act*, R.S.O. 1990, c. C.33, s. 9(3)c) and (e). Note also that this seven-year rule is also applied in Quebec in processing uniformity problems, in the absence of any Quebec text, unlike most North American jurisdictions.

[166] R.S.C. 1985, c. C-47.

a federal law may apply to the Parole Board of Canada for a "record suspension" (previously known as "pardon") in respect of that offence, after a 5-year or 10-year period (depending on the type of offence) after the completion of the sentence has elapsed.[167] Moreover, all absolute discharges are removed from the criminal record one year following the date of the sentence, while conditional discharges are removed after a period of 3 years from the date of the sentence.[168] As for demerit points which are inserted in a driver's record for traffic violations, they are usually removed from that driver's record 2 years after the date of the offence.[169]

As a general principle, under Canadian data protection laws, consent is generally required before collecting and using personal information, and an organization cannot collect or use information which is not "necessary".[170] This means, for instance, that personal information cannot be used by an organization (e.g. an employer), unless it is directly linked (and relevant) to the employees' position, or by an organization if the information is not necessary to allow that body to provide the service concerned, therefore providing for an additional protection for individuals.

Organizations also need to be cautious, under Canadian human rights laws, before collecting or using certain types of information.[171] For instance, under many provincial human rights laws, employers cannot dismiss an employee owing to the mere fact that the employee was convicted of a penal or criminal offence, if the offence is in no way connected with the employment (or if the employee has obtained a pardon for the offence, depending on the province).[172]

While these laws restricting the use of certain information may address some of the concerns raised by the RTBF, the reality is that in practice, it may be difficult for individuals to know if they were refused a given employment or any other benefit or service based on their personal information being available online. Organizations may not necessarily be transparent about the fact that they conducted online or social media searches about the individuals in question and that the information found impacted their decision. Perhaps enhancing the transparency requirement in eligibility decisions should be considered by regulators in order to address this challenge. Another aspect to consider is the fact that perhaps, as a society, the norm of what is "acceptable" will evolve over time and in light of the availability of the information on the Internet as further discussed in section 3.3.1.

---

[167] See *Criminal Records Act*, R.S.C. 1985, c. C-47, s. 3 and 4.

[168] For all absolute and conditional discharges received on after July 24, 1992. See *Criminal Records Act*, R.S.C. 1985, c. C-47, s. 6.1.

[169] See, for instance, s. 116 of the Quebec *Highway Safety Code*, which provides that "The number of demerit points entered by the Société in a person's file becomes nil two years from the date of the judgment of conviction." For Ontario, see s.1(1) O. Reg. 339/94 under *Highway Traffic Act*, R.S.O. 1990, c. H.8

[170] See s. 4.3.3 PIPEDA; s. 16 and 17 Alberta PIPA; s. 14 and 15 B.C. PIPA, s. 5 and 9 of the ARPPIPS. [See e.g., s. 7(2) B.C. PIPA; 7(2) Alberta PIPA.]

[171] *British Columbia Human Rights Code*, [RSBC 1996] chapter 210; *Alberta Human Rights Act*, R.S.A. 2000, chapter A-25.5; *The Saskatchewan Human Rights Code*, chapter S-24.1; Manitoba *The Human Rights Code*, C.C.S.M. c. H175; Ontario *Human Rights Code*, R.S.O. 1990, c. H.19; Quebec *Charter of Human Rights and Freedoms*, chapter C-12; New Brunswick *Human Rights Act*, RSNB 2011, c 171; Nova Scotia *Human Rights Act*, RSNS 1989, c 214; Prince Edward Island *Human Rights Act*; chapter H-12; and Newfoundland and Labrador *Human Rights Act*, 2010, SNL2010 Chapter 13.1.

[172] See for example the Ontario *Human Rights Code*, R.S.O. 1990, c. H.19, see s. 5 (1), 10 and 21 (1)), the British Columbia *Human Rights Code,* [RSBC 1996] Chapter 210, and the Quebec *Charter of Human Rights and Freedoms*, Chapter C-12, s 18.2.

A recent complaint under PIPEDA involving Globe24h, a Romanian-based website,[173] further illustrates yet another challenge to consider as regards the Internet making information more easily available: we might need to revisit and reconsider the extent of the availability of some of our public records. In that recent case, the website republished Canadian court and tribunal decisions and allowed them to be indexed by search engines, such that some very intimate and sensitive personal information included in these court decisions surfaced, in response to searches focusing on individuals' names.

2.2 Laws Pertaining to the Protection of Privacy and Reputation

In Canada, certain statutes (other than data protection laws) more specifically restrict the dissemination of harmful personal information: these include privacy laws and torts, as well as enactments protecting reputation.

2.2.1 Privacy and Reputation Legal Framework

Pasquale, in his recent article about reforming the law of reputation, argues that "[t]hose concerned about reputational integrity should also propose and attempt to enact legislation governing controllers and processors of data. (…) The law must be modernized, or it will fail to respond to the exact situations it was written to address."[174] As discussed in the section below, not all provinces in Canada already have a legal framework specifically addressing the privacy and reputational issues and concerns at the heart of the RTBF. A first step, for these provinces, would logically be to adopt adequate laws or amend their current legislation so as to ensure that individuals receive adequate protection, before even considering the implementation of a RTBF.

- **Privacy**

The current legislative framework in Canada, at least in some jurisdictions, may already be allowing courts to strike an appropriate balance between the right to privacy and another fundamental right, namely freedom of expression. Many Canadian provinces have laws that offer additional privacy protections, although Quebec has the most privacy-friendly legal framework in place and the most highly developed case law in this field. In Québec, the right to privacy has been elevated to the rank of a fundamental right protected by the Constitution.[175] Several pieces of legislation, including articles 3, 35 and 36 of the *Civil Code of Québec*[176] (hereinafter "C.C.Q."), protect the right to privacy. Article 35 C.C.Q., which states that "[e]very person has a right to the respect of his reputation and privacy," illustrates the principle outlined in Article 5 of the Quebec *Charter*.[177] Article 36 C.C.Q., for its part, draws up a list of acts that may be considered as invasions of a person's privacy. Paragraph 36(5) C.C.Q., in particular, specifically prohibits the use of one's "name, image, likeness or voice for a purpose *other than the legitimate information of the public*."[178]

---

[173] PIPEDA Report of Findings 2015-002, "Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA".

[174] Pasquale, *supra* note 10 at 516.

[175] Édith Deleury and Dominique Goubau, "Le droit au respect de la vie privée," in Dominique Goubau, *Le droit des personnes physiques*, 5th ed. (Cowansville, QC: Yvon Blais, 2014) at 173 [Deleury & Goubau].

[176] Chapter C-12.

[177] Deleury & Goubau, *supra* note 175 at 177.

[178] Several cases have considered this limitation and they are discussed below under section 2.2.2.

Quebec courts have characterized the right to privacy as "one of the most fundamental rights related to personality."[179] That said, as with any other right, the right to privacy is not absolute and must be balanced with other fundamental rights, including freedom of expression, since the use of one's "name, image, likeness or voice," does not extend to purposes "related to the legitimate information of the public."[180] The language "other than the legitimate information of the public" has been interpreted to mean the right to freedom of expression, freedom of the press and the public's right to information.[181]

As discussed in section 1.1.2, many common law provinces also have statutes that explicitly recognize the existence of a tort of violation of privacy. In Ontario, the tort of *intrusion upon seclusion* has been introduced very recently.[182] The provinces of British Columbia, Saskatchewan, Manitoba and Newfoundland and Labrador each have a *Privacy Act* providing that it is a tort for a person, wilfully and without a claim of right, to violate the privacy of another (which includes eavesdropping or surveillance).[183] Similar to the Quebec legal framework, each of these statutes from Canada's common law provinces also provides for exceptions or defenses in the event that the information collected or published is adjudged to be in the public interest.[184]

- **Defamation**

In the specific context of online publications, an important concern is the protection of reputation. The Supreme Court of Canada has even recognized, in a landmark case, that the protection of reputation is "intimately related" to the protection of personal privacy.[185] In the Anglo-American common law tradition, civil and criminal penalties have long been imposed for making statements that are malicious, false, and disparaging to another person or group.[186] Recovery for defamation, however, is barred if the statements are true,[187] even if they are embarrassing, and regardless of the level of malice intended by the speaker.[188]

In Canada, the protection of reputation has different ramifications, depending on the province concerned. In common law jurisdictions, "defamation law is concerned with providing recourse against *false* injurious statements, while the protection of privacy typically focuses on keeping *true* information

[179] See, e.g., *The Gazette (division Southam) v. Valiquette*, [1997] R.J.Q. 30, EYB 1996-65651 (C.A.).

[180] *Civil Code of Québec*, chapter C-12 at paragraph 36(5).

[181] *A v. Corporation Sun Media*, 2009 QCCQ 3263, at 113 [*Corporation Sun Media*].

[182] *Jones v. Tsige*, *supra* note 52.

[183] British Columbia *Privacy Act* [RSBC 1996] chapter 373; Saskatchewan *Privacy Act*, Chapter P-24; Manitoba *Privacy Act,* CCSM c. P125; Newfoundland and Labrador *Privacy Act,* RSNL 1990 chapter P-22.

[184] See s. 2(3) of the British Columbia *Privacy Act*; s. 2(3) of the British Columbia *Privacy Act*; s. 4(2) of the Saskatchewan *Privacy Act*; s. 5(f) of the Manitoba *Privacy Act*; and 5(2) of the Newfoundland and Labrador *Privacy Act*.

[185] See *Hill v. Church of Scientology of Toronto*, [1995] 2 SCR 1130 at 121.

[186] See, e.g., *Slanderous Reports Act*, 1275, 30 Edw. 1, c. 34 (Eng.); *A Brief Narrative of the Case and Tryal of John Peter Zenger*, The Historical Society of the Courts of the State of New York (1734) (establishing the precedent of truth as an absolute defense to defamation).

[187] Robert Kirk Walker, "The Right to be Forgotten" (2012), 64 Hastings Law Journal 257 at 262, discussing *The New York Times v. Sullivan*, 376 U.S. 254, 279–80 (1964); *Hustler Magazine v. Falwell*, 485 U.S. 46, 56–57 (1988); *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 345–48 (1974) and *Curtis Publ'g Co. v. Butts*, 388 U.S. 130, 164 (1967).

[188] *Ibid*.

from the public gaze."[189] The OPC has raised concerns about the limitation of these laws as a tool to address reputational harm in cases in which the harmful information published online is true.[190] It should be noted that in Québec, the accuracy of the information revealed to the public (or the fact that it is true) does not suffice to avoid civil liability.[191] In that sense, individuals' reputations are better protected with the Quebec legal framework, given that the personal information that is revealed to the public must not only be true or accurate; it must also be necessary to convey the particular content in which the public has a "legitimate interest". This type of additional layer of protection is helpful to further enhance the protection of individual reputations and should be studied by legislators in other provinces before they consider implementing a RTBF.

- **Evolving Laws: Anti-Cyberbullying and "Revenge Porn"**

Laws protecting privacy and reputation are quickly evolving. For instance, in a context where a significant number of cyberbullying and "revenge porn" acts have recently been reported, Parliament and provincial legislatures have enacted measures to address these relatively new phenomena, while courts have stepped in to fill in the gaps where necessary, notably by recognizing the existence of new common-law torts. With respect to cyberbullying, the Supreme Court of Canada, in *A.B. v. Bragg Communications Inc.*,[192] has recognized the inherent vulnerability of children and the importance of the protection of young people's privacy rights, given the extensive, direct and harmful consequences of cyberbullying. The Supreme Court even allowed one victim to proceed anonymously, in her application for an order requiring the Internet provider to disclose the identity of the relevant IP user or users.[193]

Moreover, many legislative measures have recently been enacted in order to address the issue of cyberbullying. For instance, the *Protecting Canadians from Online Crime Act*[194] (previously known as Bill C-13) has entered into force in 2014, amending the *Criminal Code* to provide, amongst other things, a new offence of non-consensual distribution of intimate images, along with complementary amendments that notably allow for the removal of intimate images from the Internet.[195] Other recent pieces of legislation such as the Manitoba *Intimate Image Protection Act,*[196] which entered into force in January 2016, also provide similar measures to address issues related to cyberbullying and "revenge porn".

Courts have also recognized the existence of other privacy-related common-law torts, notably in the context of "revenge porn". In a recent landmark decision,[197] the Ontario Superior Court of Justice explicitly recognized the existence of a new privacy tort, namely "public disclosure of embarrassing

---

[189] *Torstar*, *supra* note 42 at 59. Certain common law provinces have enacted specific laws dealing with defamation. See Ontario *Libel and Slander Act*, R.S.O. 1990, c. L.12; British Columbia *Libel and Slander Act*, [RSBC 1996] chapter 263; *Libel and Slander Act*, R.S.O. 1990, c. L.12.

[190] "Online Reputation, What are they saying about me?", *supra* note 15 at 9 and 10.

[191] See, e.g., *Société TVA inc. v. Marcotte*, 2015 QCCA 1118 at 99.

[192] *A.B. v. Bragg Communications Inc.*, [2012] 2 SCR 567, 2012 SCC 46.

[193] *Ibid,* at 31.

[194] S.C. 2014, c. 31

[195] See "Summary" section of the Act, online: <http://laws-lois.justice.gc.ca/PDF/2014_31.pdf>.

[196] SM 2015, c 42.

[197] *Doe 464533 v. N.D.*, 2016 ONSC 541.

private facts."[198] The Court also issued a permanent injunction directing the defendant to "immediately destroy any and all intimate images or recordings of the plaintiff, in whatever form they may exist, that he has in his possession, power or control," as well as another order "permanently prohibiting the defendant from publishing, posting, sharing or otherwise disclosing in any fashion any intimate images or recordings of the plaintiff."[199] This new tort will play an important role in addressing some of the reputational concerns at the heart of the RTBF. In Quebec, the Quebec Charter and the C.c.Q. are already being relied upon by plaintiffs to address revenge porn activities.[200] All of these examples illustrate how the victims of cyberbullying and revenge porn are increasingly being protected under Canadian laws, which, again, makes a stronger case against the adoption of a RTBF.

Google has decided to provide a web form on their Google.com website to enable victims of revenge porn to have it removed from search results based on their names.[201] Moreover, Google has also been active and successful in managing some situations, which are clearly illegal. For instance, mug shot extortion sites have appeared, attempting to extort money from individuals with an arrest record by publishing their photos and names, and demanding money to remove the record.[202] Google has altered its search algorithms to reduce such sites' salience.[203] Given that there is no "public interest" at stake in these types of situations, such initiatives have been welcomed and may not raise the same constitutional challenges.[204] Still, such initiatives are quite different from the implementation of a RTBF, under which Google would be in charge of deciding which content is legitimate and of public interest, and balancing the rights of freedom of information and freedom of expression in the complex area of privacy and reputational rights in Canada.

2.2.2 Balancing Rights and Determining if Information is of "Public Interest"

The CJEU case in the recent RTBF case has established a broad precedent: all European residents have the right to stop Google and other *data controllers* from linking to information deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in light of the time that had elapsed."[205] According to some, this standard lacks any objective guideposts:

> What information, which links are "irrelevant" or "inadequate?" How much time must pass and in what context? Where do media rights, self-expression

[198] *Ibid*. at 41-46.

[199] *Ibid*. at 69.

[200] In *J.G.* c. *M.B*. 2009 QCCS 2765 the defendant had transmitted to third parties intimate photos and videos of the plaintiff without the latter's implicit or explicit consent, and an amount of $39,000 was awarded in damages. In the recent case of *L.D. c. J.V.,* 2015 QCCS 1224, the Superior Court awarded $29,000 in moral damages and $3,000 in punitive damages to a plaintiff after the defendant recorded their sexual activities without her knowledge and consent.

[201] Amit Singhal, "'Revenge Porn' and Search" Google Pub. Pol'y Blog (19 June 2015), online: Google Public Policy <http://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html>.

[202] Jane E. Bobet, Note, "Mug Shots and the FOIA: Weighing the Public's Interest in Disclosure Against the Individual's Right to Privacy" (2004) 99 Cornell L. Rev. 633. *Id.* at 634–35.

[203] Barry Schwartz, "Google Launches Fix to Stop Mugshot Site from Ranking: Google's MugShot Algorithm", Search Engine Land (7 October 2013), <http://search engineland.com/google-launches-fix-to-stop-mugshot-sites-from-ranking-googles-mugshot-algori thm-173672>.

[204] See section 1.3.3 which further discusses this issue.

[205] Case C—131/12, 94.

> and free speech factor into the court's standard? What notification, if any, must Google give to websites and others that their links have been erased, or as one reporter whose blog was delisted from Google searches said, "cast into oblivion"?[206]

Google is the party in charge of interpreting the new standard. Some of the Google decisions have been compiled, contrasting successful and rejected delisting requests.[207] The result of the proposed Data Protection Regulation triggers a reverse burden of proof, requiring the organization posting the information (and not the individual claiming a right) to prove that the information should not be deleted because it is still needed or relevant. While under the current Canadian legal framework governing privacy and defamation, it is for the individual to demonstrate that the information should be removed, under the RTBF, the claimant seeking data erasure has no obligation to prove the information's irrelevancy. As discussed in section 1.3.3 as well as in section 3.1, it is not clear whether companies hosting or publishing content online will have the incentive to expend the resources necessary to demonstrate that the information is still relevant.

The law has an important role to play in ensuring that people's privacy and reputation are sufficiently protected. And indeed, to some extent, the existing framework in Canada already caters to many of the concerns underlying a RTBF. As further discussed in sections 2.1 and 2.2 above, Courts, when necessary, are the proper institutions to be charged with balancing the right to privacy and reputation against the right to freedom of information and freedom of expression. This has often proven to be a challenging and difficult task, one that has a huge impact on the fundamental rights (privacy, freedom of expression) of individuals, as well as on the value of freedom of information.[208]

As discussed above under section 2.2.1, given online reputational injuries which have become increasingly widespread, the Canadian Parliament and provincial legislatures have recently passed new laws, and Canadian courts have adopted new privacy torts, aimed at supplementing existing privacy and defamation statutes and addressing specific online problems, such as cyberbullying and revenge porn. Even the task of properly framing these laws and torts has proven to be quite a challenge. For instance and as discussed in section 1.3, the recently enacted Nova Scotia anti-cyberbullying statute was held unconstitutional and struck down by the Supreme Court of Nova Scotia in December 2015.[209]

As discussed in section 1.3.3 and in more detail in section 3.1, this complexity makes for an even stronger argument against allowing or empowering a third, private sector entity to decide these complex issues, with all the potential conflict of interests at play and the lack of any incentive to ensure that the right balance is achieved in each case and jurisdiction, in compliance with relevant legislation.

---

[206] Robert Peston, "Why has Google Cast me into Oblivion?", BBC News (2 July 2014), online: <http://www.bbc.com/news/business-28130581>, discussed in Cunningham, "The Internationalization of Censorship", *supra* note 8 at 4.

[207] Julia Powles, "Results May Vary: Border Disputes on the Frontlines of the 'Right to be Forgotten'" *Slate* (25 February 2015), online: <http://www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html>.

[208] Scassa, in her recent article, even elaborates on the fact that recent case law illustrates the difficulties faced by decision-makers in defining the scope of journalistic exceptions, particularly given the need to balance the public right to be informed against the individual's privacy rights. Scassa, *supra* note 141.

[209] *Crouch*, *supra* note 82.

In the Province of Quebec, stringent laws protecting privacy and reputation have been enacted, providing a framework that allows courts to address and determine at what point information should be considered as being a matter of public interest. Courts are in charge of striking the proper balance between privacy and reputation, on the one hand, and freedom of expression or freedom of information, on the other. The concept of bypassing this current legal framework and "giving the keys" to a private corporation allowing that corporation to decide these important societal issues should give us pause as to the reasonableness of implementing a RTBF in this jurisdiction. This is particularly true given that this province has developed a body of case law over the last twenty years, which is providing some valuable guidance on the situation in which access to certain personal information is held to be legitimate public information, and which jurisprudence, to a certain extent, has been evolving with the Internet.

- **Privacy**

The Supreme Court of Canada ruled, in *Aubry v. Éditions Vice-Versa inc.*,[210] that "[t]he public's right to information, supported by freedom of expression, places limits on the right to respect for one's private life in certain circumstances."[211] The Court explained that "[t]his is because the expectation of privacy is reduced in certain cases. A person's right to respect for his or her private life may even be limited by the public's interest in knowing about certain traits of his or her personality. In short, the public's interest in being informed is a concept that can be applied to determine whether impugned conduct oversteps the bounds of what is permitted."[212]

The Court has articulated the view that the activities of highly public figures could become a matter of public interest, in a way that the activities of ordinary individuals might not, although ordinary individuals may have their activities cast into the limelight if they are "called on to play a high-profile role in a matter within the public domain, such as an important trial, a major economic activity having an impact on the use of public funds, or an activity involving public safety." In addition, the Court reasoned that placing oneself in a public venue that is itself the subject of media attention in the public interest might result in an acceptable degree of loss of privacy as, for example, when one is caught on film at a demonstration or sporting event.[213] When assessing the appropriate balance between the right to privacy and the public's right to information, the latter being supported by freedom of expression, the Court noted: "the balancing of the rights in question depends both on the nature of the information and on the situation of those concerned. This is a question that depends on the context."[214] This view confirms that the approach to invasion of privacy focuses on the concept of public interest, which is a complex and flexible norm that has to be defined by the courts, and depending on the facts before them.

In the context of journalism, when information of a private nature is reported, courts will consider "whether the extent of disclosure of personal information was necessary to convey the particular content in which the public has a legitimate interest."[215] In *Société Radio-Canada v. Radio Sept-Îles*

[210] *Aubry*, *supra* note 45.

[211] *Ibid*. at 57.

[212] *Ibid*.

[213] *Aubry*, *supra* note 45, at 57.

[214] *Ibid.* at 58.

[215] *Ibid*.

inc.,[216] justice LeBel (then at the Québec Court of Appeal) noted that the concept of public interest is hard to define:

> It varies with the given circumstances. The concept essentially means that the dissemination of information must not be done solely to satisfy 'media voyeurism' purposes. There must be a certain level of social utility in the dissemination of that information. Otherwise, the right to privacy will be violated, which shall be punishable by law.[217]

It should be noted that Quebec courts have granted damages for unjustifiably and unreasonably republishing old information that is no longer of public interest, especially when the re-disclosure is done without reasonable justification, for example in a descriptive and sensationalist manner.[218] Some of these cases are over 100 years old. For instance, the Quebec Superior Court recognized in 1889 that the newspaper *Le Violon* was wrong to revive certain accusations which had been long forgotten about the plaintiff.[219] In *Ouellet v. Pigeon*,[220] the Court of Québec held that publishing a descriptive and sensationalist article in the newspaper *Photo-Police* concerning a murder that had taken place 10 years earlier (a woman had killed her four children and then committed suicide) could not be justified under the public's right to information, and the Court ordered the defendant to pay damages to the plaintiff.[221] In other cases, Quebec courts have found that the publication was acceptable, as the information published remained of public interest.[222] That said, it is important to point out that in all of these cases, the courts involved did not come to the abovementioned conclusion by recognizing the existence of RTBF *per se*, but rather by performing the usual balancing exercise between the right to privacy and freedom of expression, which attaches great importance to the concept of public interest. This shows that while there may be circumstances in which the unjustifiable and unreasonable re-disclosure of old information is punishable by law, such sanctions are possible under the existing legal framework.

---

[216] *Société Radio-Canada v. Radio Sept-Îles inc.*, 1994 CanLII 5883 (QC CA).

[217] *Ibid*. (free translation).

[218] See Pierre Trudel, "L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes," <http://pierretrudel.chairelrwilson.ca/cours/drt3808/Notes%20oubli3808.pdf>. This legal provision forming the basis of this right is the general extra-contractual civil liability provision found at article 1457 C.C.Q.

[219] This decision was upheld by the Court of Revision. See *Goyette c. Rodier* (1889) 20 R.L. 108,110 (C. Rév).

[220] REJB 1997-031906, 1997 (CQ) [*Ouellet*].

[221] *Ibid,* at 22. The Court ruled that by updating past events without showing any public interest in doing so, the defendants had illicitly contravened the plaintiff's right to privacy. The judge of the Quebec Court came to the conclusion that the article published by the newspaper was "sensationalist" and could not be justified by the public interest in accessing information. The judge noted that the plaintiff was the survivor of a tragedy that had taken place a relatively long time ago and that he had finally been able to rebuild his life and "forget this nightmare".

[222] See *Lévesque c. Communications Quebecor inc.*, [1999] R.R.A. 681 (since the purpose of the article was to disclose facts about the burning of the "shooting gallery" where Lévesque had once committed his crime, the information disclosed remained of public interest.) In another decision, *Mathieu c. Presse ltée (La)*, (C.Q., 1998-11-24), SOQUIJ AZ-99036093, B.E. 99BE-169, a judge from the Court of Quebec recalled that it is difficult for someone who participates in "public activities of a political nature" to invoke a right to be forgotten. The judge explained that: "he who is the main subject of a story cannot blame anyone other than himself if he did not like to be talked about." See also *Szabo c. Morissette*, (1993) R.R.A. 554.

Courts will, in some situations, take the position that the right to privacy has been infringed, even if the information published is of public interest, notably in situations where such information has been obtained by breaching the individual's privacy rights.[223]

Under the Quebec legal framework, when the photograph of an individual is published, it must be shown that the public's interest in seeing this photograph is predominant.[224] Certain courts have interpreted the notion of "legitimate information of the public" very narrowly in recent decisions,[225] which illustrates the challenge inherent in always striking the right balance. That being said, recent case law also illustrates that courts are now more and more reluctant to censor information, including pictures published on the web to illustrate an article, if the information has already been posted by the individual or is already widely available,[226] which sets a favorable precedent for freedom of expression.

The definition of the "public interest" in common law jurisdictions is generally in line with the one prevailing in Québec. In *Grant v. Torstar Corp.*,[227] Supreme Court Chief Justice McLachlin held that in order to be considered of public interest, a subject matter "must be shown to be one inviting public attention, or about which the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached."[228] Chief Justice McLachlin added that the public interest "may be a function of the prominence of the person referred to in the communication, but mere curiosity or prurient interest is not enough. Some segment of the public must have a genuine stake in knowing about the matter published."[229]

In short, by putting the emphasis on the concept of public interest, courts in both civil law and common law jurisdictions across the country have generally been able to strike an appropriate balance between two competing rights, namely the right to privacy and freedom of expression. In case of conflict between these two fundamental rights, the solution may be found in the notion of *public interest*, given

---

[223] *Corporation Sun Media, supra* note 181.

[224] In *Gazette (The) c. Goulet*, 2012 QCCA 1085, the appellants used a file photo identifying the respondent in uniform standing in the doorway of the penitentiary he guards, in order to illustrate an article about the opposition of neighboring citizens to an expansion of the building housing the prison project, and the trial judge concluded that the image of the respondent was of no relevance to the content of the message thus transmitted. The same reasoning has been applied in other decisions. See, for instance, *Bloc v. Sourour*, 2009 QCCA 942.

[225] See *Hammedi c. Cristea*, 2014 QCCS 4564 (CanLII). Pierre Trudel has raised concerns over the restrictive position the Court took in this decision on the issue of what constitutes legitimate information of the public, and expressing the view that pictures play a significant role in informing the public. Pierre Trudel, ''Portée excessive du droit à l'image'', *Journal de Montréal* (25 September 2014); See also Eloïse Gratton, ''A picture is worth a thousand words'', (26 Septembre 2014), online at: <http://www.eloisegratton.com/blog/2014/09/26/a-picture-is-worth-a-thousand-words/>; Leonid Sirota, ''Une image et mille maux'' (10 October 2014), online at: <https://doubleaspectblog.wordpress.com/2014/10/10/une-image-et-mille-maux/>. See also *Pia Grillo c. Google inc*., 2014 QCCQ 9394.

[226] *Blanc c. Editions Bang Bang*, 2011 QCCS 2624. In this case, the Superior Court held that Ms. Blanc, a public personality, had tacitly consented to the use of her picture by using it online on her blogs, on Facebook and on Twitter. See also *Amin c. Journal de Montréal,* 2015 QCCQ 5799, in which a Quebec judge also considered the importance of freedom of expression in a similar case and ruled that although there was no doubt that the defendant intended to criticize severely and firmly the veiling of young Muslim girls and, more specifically, their participation in certain competitions, the Court took the view that these pictures were part of the public domain and that, as such, they could be reproduced by a newspaper.

[227] *Torstar*, *supra* note 42.

[228] *Ibid.* at 105.

[229] *Ibid*.

that the latter allows courts to determine whether the public has a genuine stake in knowing about the private information that is being revealed to the public.[230]

- **Defamation**

In reputation and defamation claims, courts first need to determine if the online publisher of the information committed a fault in publishing the information. This may be the case if the facts alleged in the publication were untrue (although, as mentioned in section 2.2.1, in Quebec, it is not because facts are true that an action in defamation will automatically be rejected), and the court would also take into account the spirit of the author and the overall publication (was it done to harm the subject of the posting?). The court will look at various factors, including the background of the author, the whole context of the posting, the circumstances leading to this blog, etc.[231] Several decisions have also been rendered by courts whereby a defendant has been ordered to pay damages for harm to the plaintiff's reputation and invasion of his or her privacy, because of texts published on the Internet.[232] The type of damages awarded depends on the comments posted, and the damages are usually linked to the availability of the comments, and the number of individuals who had access to the documents.[233]

Canadian courts have repeatedly recalled that freedom of expression is the cornerstone of a free and democratic society and that the right to reputation and the right to privacy may, in some cases, be justifiably violated in the name of democracy.[234] The more an online publication relates to significant political issues, the more broadly the rights to freedom of opinion and expression are interpreted.[235] Consequently, even if there is no hierarchy of rights and freedoms protected by either the Canadian or the Quebec Charter, courts may, depending on the context, prioritize certain rights for the collective well-being. For instance, where the right to reputation is opposed to freedom of information in the context of a blog published on social media, the Superior Court of Quebec recently followed the Supreme Court's reasoning in *Crookes v. Newton*,[236] where it cited an excerpt from author Lyrissa Barnett Lidsky to the effect that "the problem for libel law, then, is how to protect reputation without squelching the potential of the Internet as a medium of public discourse."

[230] See *Torstar*, *supra* note 42 at 102.

[231] *Ibid*.

[232] For cases from common law jurisdictions, see e.g. *Barrick Gold Corporation v. Lopehandia et al.* (2004), 2004 CanLII 12938 (ON CA), 71 O.R. (3d) 416 (C.A.), where the Ontario Court of Appeal awarded $75,000 as general damages for defamatory and malicious statements published on the Internet; See also *Kumar v. Khurana*, 2015 ONSC 7858.

[233] See *Laforest v. Collins* 2012 QCCS 3078 [*Laforest*]. In *Davis c. Singerman*, 2014 QCCS 70 (CanLII), an amount of $5,000 was awarded to compensate moral damages suffered by the Plaintiff after a message posted on her Facebook account was accessed by 18 individuals; In the case of *Lapierre v. Sormany* EYB 2012-210900 (C.S.), Justice Yergeau awarded general damages in the amount of $20,000 for a Facebook publication available to general Facebook users over a period of 4 days; In *Carpentier v. Tremblay* EYB 2013-217223 (C.Q.), Justice Bérubé awarded a sum of $5,000 to the victim of a Facebook comment available to 42 individuals over 2 weeks; In another case concerning the vindictive behavior of an individual who published various derogatory comments on Facebook, *Lapointe c. Gagnon* EYB 2013-218181 (C.Q.), the Court awarded $8,000 as general damages. It was shown that the comments became known by co-workers of the Plaintiff; In the case of *9080-5128 Québec inc. c. Morin-Ogilvy,* 2012 QCCS 1464 (CanLII), Justice Langlois awarded general damages of $4,000 to one Plaintiff for comments made available to 426 individuals on Facebook, over a period of 2 days. The evidence showed the comments were most likely seen by only a few users.

[234] *Bou Malhab v. Diffusion Métromédia CMR inc.*, *supra* note 168; See also *Rosenberg v. Lacerte*, 2013 QCCS 6286 [*Rosenberg*].

[235] *Lafferty, Harwood & Partners c. Parizeau et al.*, [2003] CanLII 32941 (QC CA), par. 155; *Rosenberg, supra* note 234 at para 141.

[236] *Crookes*, *supra* note 73, at para 37.

The OPC has mentioned, in its recent research paper pertaining to online reputation, having investigated a case pertaining to impersonation and reputational harm,[237] where a mother complained that someone had created a Facebook account in her teenaged daughter's name. The imposter contacted her daughter's friends and made inappropriate comments about them. It should be noted that over the last few years, some Quebec plaintiffs, relying on the C.C.Q. and the Quebec *Charter*, have been successful in impersonation lawsuits over fake Facebook profiles.[238] In common law Canada, a similar action may be brought, invoking the tort of appropriation of personality.[239]

There are, however, some limits to the efficiency of these laws in addressing the concerns which a RTBF attempts to address. As the OPC has mentioned: "once information has been posted online, there is never any guarantee that it has not been reposted elsewhere on the Internet."[240] In *Laforest v. Collins*,[241] in order to address that concern (that the negative comments could be reposted elsewhere on the Internet), the Superior Court of Québec ordered the defendant to write and sign a letter of withdrawal, whereby she would confirm that the negative comments about Laforest were untrue. In the event that the defendant contravened her undertaking of not publishing any further negative comments about him, or if the offensive comments were eventually found on other websites, Laforest was authorized, in advance, to publish the said letter, using a similar means of communication, thus allowing him to reach an equivalent number of people who might have viewed the negative comments.[242] This type of order may become increasingly useful in future online defamation cases.

The OPC has also pointed out that there are significant limitations to judicial recourses. For instance, the OPC has raised the point that the cost of pursuing litigation may not make this type of remedy accessible for everyone.[243] Perhaps these types of concerns should be considered by regulators. For instance, the possibility of developing a simpler, cheaper and faster process for these types of requests for online content removal could ensure that the current legal framework would work more effectively in protecting the individual's reputation and privacy rights, without the need to import a RTBF, with its inherent downsides and constitutional challenges.

2.3 Laws Regulating Intermediaries and Takedown Procedural Tools

Another consideration that militates against the importation of a RTBF in Canada is the fact that there are already several legal and procedural mechanisms in place and available to individuals in order to allow them to request the removal of harmful information or content posted online or on other platforms. First, laws have been enacted in order to regulate web intermediaries and service providers, and to provide a certain level of protection against illicit information posted on the Internet. Secondly, takedown procedural tools are already in place in most jurisdictions to allow individuals to obtain information about the authors of illicit content posted about them online and have such content removed.

---

[237] See PIPEDA Report of Findings 2013-010.

[238] See for example *Laliberté c. Transit Éditeur inc.*, 2009 QCCS 6177 and *A.c.B.*, 2009 QCCQ 14676 (CanLII).

[239] Teresa Scassa and Michael Deturbide, *Electronic Commerce and Internet Law in Canada*, 2nd Edition, CCH Canada, at 342. See also *R.C. Simoes*, 2014 ONCA 144 (CanLII).

[240] "Online Reputation, What are they saying about me?", *supra* note 15, at 6.

[241] *Laforest, supra* note 233.

[242] *Ibid,* at paragraph 170.

[243] "Online Reputation, What are they saying about me?", *supra* note 15, at 9 and 10.

2.3.1 Laws Regulating Intermediaries

The current legislative framework in Canada already provides protection against illicit information posted on the Internet, defamation and other potential harm, although the extent of this framework depends on each jurisdiction, with the Province of Québec having the most stringent one. In Québec, in addition to the provisions of the C.C.Q. and the Quebec Charter referred to above, the *Act to Establish a Legal Framework for Information Technology*[244] (hereinafter "AELFIT") provides for a certain level of protection against illicit information posted online. For instance, section 22 of the AELFIT provides that a service provider may incur responsibility if, upon becoming aware that the content it hosts or makes available is being used for an illicit activity, it does not act promptly to block access to that content or to otherwise prevent the pursuit of the activity.[245] While there is little case law regarding this provision, notably regarding the meaning of "illicit," it nonetheless establishes, in conjunction with the general principles of civil liability set forth in the C.C.Q., a liability regime under which a person who believes himself or herself to be a victim of defamation can petition the court having jurisdiction to order a webpage to be taken down (in the case of a web host) or a hyperlink to be removed (in the case of a search engine).

That said, according to Professor Trudel, a service provider that has been notified of the existence of an illicit document should be entitled, before taking down a webpage or removing hyperlinks, to seek confirmation or evaluation from a third party, such as a neutral expert, who would determine whether the impugned document was actually illicit or not.[246] In other words, as long as a web intermediary does not receive an independent confirmation of the illicit character of a document posted online, it would not be under any obligation to promptly censor the information.[247] For Trudel, such an approach would be in line with the principles regarding freedom of expression and the public's right to information.[248] The power to take down pages or to remove hyperlinks is an important one, which should be taken seriously, given the possible adverse effects on freedom of expression and the general availability of information. In any case, it is debatable whether any service provider or any other private entity such as Google could ever be considered as a neutral third party possessing the necessary expertise in this context.

In common law provinces, while case law makes it clear that an Internet search provider is not a publisher of defamatory material identified or contained in its search results,[249] individuals have other means at their disposal to have webpages or links to offending or defamatory posts removed by service providers. These means include defamation proceedings against service providers. For instance, in *Canadian National Railway Company v. Google Inc.*,[250] the plaintiff sought and obtained a removal order in respect of a blog hosted by Blogspot, a Google subsidiary, on the grounds that it contained defamatory material. Google first blocked the site, on a temporary basis, but later announced that it was

---

[244] Chapter C.-1.1.

[245] *An Act to establish a legal framework for information technology*, ch. C-1.1, s. 22.

[246] See Pierre Trudel, "La responsabilité sur Internet en droit civil québécois" (13 June 2008) online : <http://www.pierretrudel.net/files/sites/6/2015/01/TRUDEL_resp_internet.pdf> at 1.

[247] *Ibid*.

[248] *Ibid*.

[249] *Crookes*, *supra* note 73.

[250] *Canadian National Railway Company v. Google Inc.*, 2010 ONSC 3121.

"no longer prepared to block or agree to the removal of the site without a 'prompt' court order," which it did not oppose.[251] This decision from the Ontario Superior Court of Justice is interesting on a least two levels. On the one hand, it shows that individuals do in fact have the power to seek and obtain removal orders from courts with respect to defamatory material posted online, including on blogs or weblogs. On the other hand, the decision also illustrates how important it is to leave to courts the task of determining whether certain content is defamatory or not. Indeed, as illustrated by the fact that Google did not oppose the court order, service providers have little interest in keeping a website online, especially when they are aware that they could be held liable for defamation and damages, which in turn raises questions about the status of freedom of expression in our society. To put it differently, leaving the determination of what constitutes online defamation to the sole discretion of service providers and other private actors could seriously restrict the flow of information and freedom of expression, given that these private actors have little or no incentive to keep this content online – especially when they have a defamation lawsuit hanging over their heads like the sword of Damocles.

In the same vein, courts are in a better position than private actors to properly balance the public's interest in protecting freedom of expression and an individual's interest in protecting his or her reputation in the context of Internet publications. In 2011, the Supreme Court of Canada rendered an important decision regarding hyperlinking.[252] The Court held that hyperlinking, in and of itself, should never be seen as "publication" of the content to which it refers. Justice Abella, writing for the majority, was wary of the risk of the potential "chill" effect for primary article authors: "Limiting [the] usefulness [of hyperlinks] by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression." However, the Court noted that hyperlinking could attract liability in certain circumstances, notably where a person uses a reference in a manner that in itself conveys defamatory meaning against another person.[253] It is not clear if such a balanced approach would have been considered in a context where the decision whether a website should be taken down or a hyperlink removed is left to a private sector organization that may not necessarily have the same level of expertise and independence that courts have.

2.3.2 Take Down Procedures

In the current legal framework, individuals, in addition to the legal provisions mentioned above, also have certain procedural tools at their disposal to have webpages taken down or links to offending or defamatory posts removed by service providers.

First, it is common practice to start by sending a demand letter to the author of the document (or to the person responsible for the dissemination of information) in order to allow them to remove the content themselves voluntarily. Should the author of the document (or the person responsible for the dissemination of information) refuse to comply, the aggrieved party can then file an injunction petition, in order to force the author to do so, or can claim moral and punitive damages.

Following these steps, it is often advisable to contact the owner of the Internet domain, in order to request removal of the information from the website that the owner is hosting. Refusal to comply with

[251] *Ibid.*, at paras 5-6.

[252] *Crookes*, *supra* note 73. See also section 1.3.1 of this paper which discusses these issues.

[253] *Ibid*. at 40.

such request may render the owner liable for damages for contributing to the dissemination of false information.

In a case where the author of the information is unknown, as it is often the case on the Web, it is also possible to obtain a court order, such as a Norwich order (an equitable remedy that permits a court to order discovery of a person who is not a party to the contemplated litigation),[254] forcing an Internet service provider to reveal information pertaining to the IP address from which the false or defamatory information is diffused.[255] This often allows the affected individual to identify the author of the false or defamatory information or the person responsible for its dissemination, and allows for the institution of proceedings against that person.

In conclusion, we believe these measures to be very efficient, since their application would force a case-by-case analysis of the limits to freedom of expression, and, because successful application of the measures would see the impugned information totally removed from the Internet instead of its reference in a search engine simply being removed. In addition and as discussed above under section 2.2.1, the individual concerned can still claim damages, in cases in which the comments infringed his or her privacy or reputation.

In short, the current legal framework in both civil law and common law jurisdictions already provides for a useful level of protection against illicit or defamatory information posted on the Internet. While there is little jurisprudence on this relatively new topic, the legal framework in place in Canada and especially in Quebec grants adequate protection against illicit or defamatory information being posted or hosted by a service provider, especially when the latter has been duly notified of the existence of the impugned content. As already noted above, the challenges in practice may include the costs and time associated with exercising this removal right, and therefore perhaps a faster, easier and more accessible process could be considered.

The OPC, in its recent paper on Online Reputation, explains how one of the biggest challenges for the OPC in dealing with issues of online reputation has been asserting jurisdiction over the sites that come to our attention, particularly when they are based outside of Canada.[256] As a matter of fact, in those circumstances, there may not always be a real and substantial connection to Canada, which is required in order for a foreign-based organization to be subject to PIPEDA. This being said, the OPC mentions that in cases where the OPC's jurisdiction was established, it has generally been successful in having information removed from organizations' websites.[257] The Global Privacy Enforcement Network (GPEN), a group of privacy regulators whose mission is to improve cooperation in enforcement of cross-border laws affecting privacy, may play an important role in addressing these types of concerns. It was formed in 2010, in response to an OECD Recommendation on Cross-border Cooperation in the Enforcement of

[254] See the seminal case *Norwich Pharmacal Co*. v. *Customs and Excise Commissioners*, [1974] A.C. 133. In Canada, the leading case is *Glaxo Wellcome PLC* v. *M.N.R*., [1998] 4 C.F. 439, leave to appeal refused, [1998] S.C.C.A. No. 422. See also *BMG Canada Inc*. v. *John Doe*, 2005 FCA 193.

[255] See for instance *York University* v. *Bell Canada Enterprises*, 2009 CarswellOnt 5206 (Ont. S.C.J.). See also *Hogan* v. *Great Central Publishing Ltd*., 16 O.R. (3d) 808 (Ont. Gen. Div.) and *Irwin Toy Ltd*. v. *Joe Doe*, [2000] O.J. No. 3318 (Ont. S.C.J.).

[256] "Online Reputation, What are they saying about me?", *supra* note 15, at 6.

[257] *Ibid*.

Laws Protecting Privacy.[258] These types of initiatives will be increasingly important to ensure the enforcement of courts' orders pertaining to online privacy and reputations rights.

[258] Members include privacy authorities from Australia, Belgium, Bulgaria, Canada, Macau SAR (China), Czech Republic, Estonia, France, Germany, Guernsey, Ireland, Israel, Italy, Korea, Mexico, Netherlands, New Zealand, Norway, Poland, Slovenia, Spain, Switzerland, Ukraine, United Kingdom, the United States and the European Union.

3. PRACTICAL REASONS THAT ARGUE AGAINST A RTBF FOR CANADA

In previous sections of this paper, we have discussed the reasons why a RTBF would not be acceptable in Canada due to serious legal and constitutional concerns (section 1) and the fact that we may not even need such RTBF, considering that some of our laws already provide for an adequate framework (section 2). In this section 3, we provide a review of the practical reasons that make a RTBF impossible to implement without serious harms to a wide range of societal interests. In particular, we consider other rights that would be affected, such as the fundamental right of freedom of expression, as well as the right to access to information and to equal rights and opportunities. We have reviewed how the interpretation of the RTBF according to Court of Justice of the European Union in the *Google Spain* decision[259] has led to censorship, infringements of freedom of expression, as well as outsourcing to corporate decision-makers the duty of balancing fundamental rights.

3.1 Challenges with Outsourcing the Right to be Forgotten

As of the writing of this paper, Google has reported having received over 405,305 takedown requests covering over 1.4 million URLs.[260] Google has agreed to remove links in approximately 42% of those cases. According to its website, Google takes into account a number of considerations in deciding whether to comply with a takedown request.[261] The lack of a recourse mechanism and independent oversight (which is discussed in sections 1 and 2) has also been raised as another concern.[262]

But there is another concern with the proposed RTBF and Oxford Professor Floridi summarizes it well: "a private company now has to decide what is in the public interest."[263] Members of the United Kingdom's House of Lords have articulated the view that it is wrong to leave it to search engines to decide whether or not to delete information, based on vague criteria.[264] Google's role as the *de facto* decision-maker of these value-laden societal issues is raising much concern, especially since Google has even admitted to be struggling with implementing the ruling.[265] Google has also publicly confessed missteps in its attempted compliance.[266]

---

[259] *Google Spain SL, supra* note 3.

[260] Google, "Transparency Report", *supra* note 11.

[261] Google, "Letter from Google to the Article 29 Working Party", *supra* note 12.

[262] *Ibid.*

[263] Caroline Preece, Rosie Clarke, "Google 'Right to be Forgotten': Everything You Need to Know", *ITPro* (9 February 2015), online: ITPro <http://www.itpro.co.uk/security/22378/google-right-to-beforgotten-everything-you-need-to-know> (quoting Professor Luciano Floridi).

[264] Catherine Baksi, "Right To Be Forgotten "Must Go", Lords Committee Says", *Law Gazette* (30 July 2014), <http://www.lawgazette.co.uk/law/right-to-be-forgotten-mustgolordscommittee-says/5042439>.

[265] Computerworld, "This is how Google handles 'Right to be forgotten' requests", *Computerworld* (19 November 2014), online: Computerworld at <http://www.computerworld.com/article/2849686/this-is-how-google-handles-right-to-be-forgotten-requests.html>. Right after the decision, Google had even convened an *Advisory Council to Google on the Right to Be Forgotten*, at <https://www.google.com/advisorycouncil/> discussed in "Online Reputation, What are they saying about me?", *supra* note 15 at 5.

[266] See Caroline Preece, Rosie Clarke, "Google 'Right to be Forgotten': Everything You Need to Know", *ITPro* (9 February 2015), online: ITPro <http://www.itpro.co.uk/security/22378/google-right-tobe-forgotten-everything-you-need-to-know> (quoting Google's chief legal officer as saying "Only two months in, our process is still very much a work in progress. It's why we incorrectly removed links to an article last week."), a topic discussed in Cunningham, "The Internationalization of Censorship", *supra* note 8 at 28-29.

Under the RTBF, search engines as private companies must unilaterally determine the balance between the value of information being published and the impact on a user. This raises various challenges which are discussed below.

3.1.1 Search Engines Unilaterally Balancing Rights

Section 2.2.2 of this paper discusses how Courts are the proper institutions, in Canada, to be charged with balancing the right to privacy and reputation against the right to freedom of information and freedom of expression, although this has often proven to be a challenging and difficult task. As discussed by Professor Trudel, the notion of "public interest" is a complex and evolving notion:

> Public interest is also a concept defined in many different domains of human thought and action: morality, ideology, commonly held or accepted beliefs, as well as perceptions and fantasies that are more or less widespread throughout civil society – in short, the common sense of the period concerned and the moral standards ingrained in the whole body politic. No source of law, not even legislation, can exert any enduring influence over the emergence of concepts and attitudes that spontaneously combine, clash and then coalesce once more. Refining the reasoning, concepts and conceptions that go into determining what the public is entitled, or has a legitimate interest, to know requires maintaining a vibrant community in which differing conceptions can confront one another vigorously.[267] (free translation)

Google is not an administrative tribunal exercising the quasi-judicial role of deciding the fate of the public interest in accessing certain information in Canada.[268] The decision as to whether a specific piece of information that is published has value to the public that is greater than any harm it may cause to an effected individual is often a complex one, as further discussed in section 2.2.2. To evaluate this decision, an expert must understand the nature of the content, examine the potential audiences that might deem it useful, assess the credibility and quality of the content and understand whether it might help provide information that would supplement or add bits of information to a research that would otherwise be incomplete. The expert must then investigate whether the figure affected is a public figure, whether the information about the figure is relevant to some broader audience that has reason to be interested in this individual and any specific facts and circumstances about the situation at hand. It is clearly impossible for a private corporation to take on such investigations for what can amount to millions of user requests.

We can review the implementation of the RTBF in Europe and see how these factors are indeed resulting in practical concerns. We note that those seeking the removal of search results which they wish to delete are not incented to provide both sides of the story, as they only advocate to remove data. Search engines in Europe accordingly must rely only on the basis provided by reading the information and the complaint. But to assess whether the individual is a public figure or whether the data is "relevant" is a complex investigation, search engines, to do this effectively, would need to research the background of each case – which in many cases cannot be done without interviewing the publisher or investigating facts on the ground. Many complaints would need an investigative team to conduct research and determine whether data is accurate or up to date.

---

[267] See Pierre Trudel, "L'oubli en tant que droit et obligation dans les systèmes juridiques civilistes," *supra* note 218.

[268] See section 1.3.3 which elaborates on this issue.

As further discussed under section 1.3.3 entitled "Minimal Impairment," adding to allegations of censorship, data controllers have no obligation under either the CJEU case or the Directive 95/46/EC to alert webmasters that links to their pages have been delisted,[269] and it has been alleged that E.U. officials were even discouraging Google from giving such notices.[270] In most cases, the most informed advocate for why information should be available is the publisher of the content. The publisher has made the editorial decision that this content is valuable enough to the public to be published and has the facts and circumstances to weigh the countervailing issues. Those concerns are already balanced by legal judgements about privacy rights and free expression. Search engines rely on the decision to publish or remove such content as basic evidence that such information is legally available. Search engines from their position removed from direct publication are thus forced to make a secondary assessment, without any knowledge, that this content about an individual must be practically inaccessible via a search for that individual's name.

Sometimes, the relevance of certain information may be triggered by a researcher, who uses search engines to investigate a pattern or an important issue. Search engines cannot predict whether a public health researcher or a family member researching his ancestors will find certain information relevant or not. These results will be hidden from researchers who may have a compelling need to access data that could yield great societal value.

3.1.2 Decision on Retention and Restoring Data

At what point does relevant data become less important to the public than the harm it causes to an individual? The "correct" retention time frame for search results is unknown and uncharted, and is thus impossible for a corporation to assess. The RTBF assumes that certain data that may have been valuable and relevant at one time becomes less so and must be deleted at some point. However, there is no guidance available that would shape the decisions of a private corporation forced to delete data.

These decisions, such as when the commission of a certain type of crime should be unavailable via search are the mandate of policymakers, not the intuition of a corporation's employees. Consider the now famous example of data about the Spanish debtor at issue in the Court of Justice. At exactly what point did his debts age to the point that they become not relevant to display in search results, but yet to stay available where published? Were they ever worthy enough of search availability? Only policymakers or the judiciary can make this determination. As further discussed in section 1.3.3, another challenge is to determine, for instance, what sort of public role would have made our debtors data worthy of longer availability. Perhaps if he was an elected official? A local political party functionary? A government official? Or an accountant? Perhaps he would be considered as a public figure if he was a famous actor, but what if he acted only in local amateur shows? Outsourcing such decisions to the private sector means handing over governments' complex public policy role to corporate decision-makers. Only the Courts and government authorities are in the best position to assess whether certain material should be delisted, according to specific circumstances and applicable laws, as they have the procedural means to guarantee fairness and the right to audience of both sides.

---

[269] *Google Spain SL*, *supra* note 3; but see General Data Protection Regulation, *supra* note 2, art. 17 (requiring data controllers to notify third parties of requested deletions).

[270] See Jeffrey Toobin, "The Solace of Oblivion", *supra* note 9 (29 September 2014) (citing objections from the Article 29 Working Party to "Google's practice of informing publishers when links that individuals objected to were deleted"), a topic discussed in Cunningham, "The Internationalization of Censorship", *supra* note 8 at 27.

In her new book, *Ctrl+Z: The Right to be Forgotten*, Georgetown University Assistant Professor Leta Jones explains that "when information is made public, a court or agency order should be required for right-to-be-forgotten removal requests."[271] In her opinion, intermediaries are far from the optimal party to be assessing oblivion claims. She explains:

> The parties in the best position to assess the needs of the data controller, the subject, and the public are data-protection agencies or, at a minimum, the data sources themselves. Although the source of the content knows the context and justifications for the communication far better than an intermediary like Google does, the source may still just remove the content upon request to avoid any legal issues. It is best if users request oblivion through DPAs, which may continue to make these assessments in line with their evolving domestic laws. The DPAs are in best position to assess the many needs at issue, are engaged with the public, and are paid to develop laws.

Another substantial issue that makes the RTBF impractical is that some content that is considered irrelevant in the present, might become relevant in the future. Who should be the party responsible to advocate restoring content that becomes relevant once again? If an individual enters the political sphere, and evidence of his misdeeds are important to voters, who identifies and restores the availability of results that were deleted? At the time that the information might be most relevant, where voters or researchers seek to assess the merits of an emerging public figure, data will be unavailable.

As suggested by Professor Floridi, the RTBF is a half-baked solution, and "If Europe really wanted to regain control over personal data, giving Google this type of power is an odd outcome."[272]

3.2 Censorship and Value of Freedom of Information

One of the most repeated arguments against a 'right to be forgotten' is that it would constitute a concealed form of censorship.[273] As Ausloos explains:

> By allowing people to remove their personal data at will, important information might become inaccessible, incomplete and/or misrepresentative of reality. There might be a great public interest in the remembrance of information. One never knows what information might become useful in the future. Culture is memory. More specifically, the implementation of a fully-fledged 'right to be forgotten' might conflict with other fundamental rights such as freedom of expression and access to information. Which right should prevail when and who should make this decision? Finally, defamation and privacy laws around the globe are already massively abused to censor legitimate speech. The introduction of a 'right to be forgotten', arguably, adds yet another censoring opportunity.[274]

---

[271] Meg Leta Jones, *Ctrl+Z: The Right to be Forgotten* (New York; London: New York University Press, 2016) at 179 [Jones].

[272] See Mark Scott, "Europe Tried to Rein In Google. It Backfired.", *The New York Times* (18 April 2016), online: <http://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html?_r=1>.

[273] Peter Fleischer, "Foggy Thinking about the Right to Oblivion" (9 March 2011), online: Privacy…? <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html>.

[274] Jef Ausloos, "The 'Right to Be Forgotten' – Worth Remembering?" 28:2 *Computer Law & Security Review* 143, available online at: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1970392> at 7.

The consequences of this censoring opportunity are threefold. First, from a data controller's standpoint, compliance with a RTBF may prove burdensome in practice. As a consequence, the RTBF could have a chilling effect on data controllers or other service providers who might want to avoid liability by over-blocking content (section 3.2.1). Second, the introduction of a RTBF could have a negative impact on the availability of important material online, including historical material (section 3.2.2). Finally, the introduction of a RTBF would create an unequal access to information, given that Canadian users would have access to a smaller amount of information as compared to their neighbours from the United States (or as compared to other Canadians who have access to certain tools that allow them to bypass geographical restrictions) (section 3.2.3).

3.2.1 Over-blocking as a Result of the RTBF

If companies risk liability for not removing results objected to by complainants, the certain result will be an over readiness to remove content to avoid this liability. Although Google appears to have devoted tremendous resources to its review process, buttressed by a clear corporate commitment to maximum support for free speech that seeks to maintain content that is relevant, few will risk the liability when faced with potential fines and penalties for not removing much content immediately open objection by users.

As highlighted by Professor Rosen, "Europe's top court ruling that forces Internet search engines to remove links containing embarrassing material about an individual's past may have significant implications on the future of freedom of speech online".[275] Professor Rosen says that because the tech companies cannot know in advance whether or not a particular request is going to be granted, they'll have an incentive to remove material any time anyone requests it, because otherwise they could potentially be financially liable. Rosen adds that this has the potential to change Google from a neutral search engine to a "*censor-in chief*" and arbiter of what information is relevant or damaging.[276]

Those who support a RTBF sometimes argue that companies have been able to comply with copyright law which requires a notice and takedown type procedure in the U.S.[277] Indeed, this comparison to copyright is worth further scrutiny. The United States copyright laws and other common law systems include the doctrine of fair use that permits limited use of copyrighted material without acquiring permission from the rights holders, as it is considered an exception to content owners' rights under copyright law. Relying on this legal right, individuals often post music, video or other content to public sites for a wide range of purposes, many of which are protected by fair uses. Copyright owners send publishers take down notices to object to content they claim is unlawfully posted. But in many cases, the assessment of whether a particular posting is protected by fair use is complex. There is no guarantee that certain use will qualify as fair since there is a significant grey area in which fair use may or may not apply.[278] Although many companies have worked hard to set up processes that cooperate with the obligation to respond to take down notices, while respecting fair use rights, they face liability if they do not cooperate or make the wrong decisions. Fair use advocates believe that companies prefer to avoid

[275] Marc Gollom, "Google looms as 'censor-in-chief' after 'right to be forgotten' ruling", *CBC News* (14 May 2014) online: <http://www.cbc.ca/news/world/google-looms-as-censor-in-chief-after-right-to-be-forgotten-ruling-1.2641714>.

[276] PRI and WNYC, "Should we have the 'right to be forgotten' online?" *WNYC* (13 May 2014) online: <http://www.wnyc.org/story/should-we-have-right-be-forgotten-online/>.

[277] Jeffrey Toobin, "The Solace of Oblivion", *supra* note 9.

[278] Richard Stim, *Getting Permission*, 5th ed., (NOLO, 2013), online: <http://fairuse.stanford.edu/overview/fair-use/disagreements-over-fair-use-when-are-you-likely-to-get-sued/>.

liability and quickly take down legal content, and thus tread on the rights of those posting contentWordpress.com has stated that "[t]his isn't just an outlier case; given our unique vantage point, we see an alarming number of businesses attempt to use the DMCA takedown process to wipe criticism of their company off the Internet."[279] The concerns of the fair use advocates provide a serious caution for a system that would similarly have search engine having to make a choice between liability and defending inclusion of results.

3.2.2 Right to History

Tim John Berners-Lee, the creator of the *World Wide Web*, has stated that, at present, the introduction of a RTBF seems dangerous as it can undermine the right to history, and the right to freedom of expression and freedom of information.[280] He defends the freedom of the Internet and considers that it should be protected against the threat of governments and corporations interested in controlling the web. In his opinion, Internet should be a "neutral medium" in order to reflect all of humanity, including "some ghastly stuff." In his view, the problem should be addressed from another perspective, perhaps by implementing rules that protect people from the inappropriate use of old information and also considering a neutral approach. In his own words, "now some things are of course just illegal, child pornography, fraud, telling someone how to rob a bank, that's illegal before the web and it's illegal after the web."[281]

Likewise, Jimmy Wales, founder of Wikipedia has spoken out on different occasions against the controversial *Google Spain* decision describing the RTBF as "deeply immoral."[282] In his opinion, history is a human right and one of the worst things that a person can do is attempt to use force to silence another or in his understanding, try to suppress the truth. Since the *Google Spain* decision, Wikimedia Foundation has received multiple notices of intent to remove Wikipedia content from European search results, and has decided to release a list of these notices received from search engines in one of their pages.[283]

Leta Jones highlighted that the *Google Spain* decision has important questions of scope as well.[284] She explains that after the decision was issued, there were concerns of whether blogs, news sites, social networking sites and personal websites would be next. The European Commission responded to these concerns with some public materials to help clarify the decision and its impact.[285] The European

---

[279] Paul Sieminski, "Corporations abusing copyright laws are ruining the web for everyone", *Wired* (17 May 2014), online: <http://www.wired.com/2014/01/internet-companies-care-fair-use/>.

[280] Stephen Shankland, "Web founder: Europe's right to be forgotten rule is dangerous" *CNET* (10 December 2014), online: <http://www.cnet.com/news/web-founder-europes-right-to-be-forgotten-rule-is-dangerous/>.

[281] Agence France-Presse, "Tim Berners-Lee calls for internet bill of rights to ensure greater privacy", *The Guardian* (27 September 2014), online: <https://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy>.

[282] Sophie Curtis and Alice Philipson "Wikipedia founder: EU's Right to be forgotten is 'deeply immoral", *The Telegraph* (6 August 2014), online: <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html>.

[283] Wikimedia Foundation, "Notices received from search engines", online: <https://wikimediafoundation.org/wiki/Notices_received_from_search_engines>.

[284] Jones, *supra* note 271 at 171.

[285] European Commission, "Myth-Busting: The Court of Justice of the EU and the "Right to be Forgotten", online: <http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf

Commission explained that the Court's judgment only concerned the RTBF regarding search engines' results involving a person's name, which means that the content remained unaffected in its original location on the Internet, but also that the content can still be found through the same search engine based on a different query. However, the logic of this view is difficult to understand, as powerful search tools can be used across social media web sites, large groups of blog publishers, specialized people search tools and so on. Searching today can be done by many other sources beyond search engines, such as using social media tools. Even publishers themselves can provide search tools that work across many sources.

Moreover, according to the Article 29 of Working Party's guidelines released in November 2014, for implementing the *Google Spain* decision, interpretations should be made within existing national law.[286] This interpretation resulted in inconsistent outcomes across the EU. Leta Jones explains some of these situations: "Google removed links connecting British individuals to their convictions but not those of Swiss individuals, and a district court in Amsterdam decided that Google did not need to delete the data because 'negative publicity as a result of serious crime in general is accurate permanent relevant information about a person'."[287] The guidelines provide a set of criteria for data-protection authorities handling right-to-be-forgotten complaints to follow, but some of the questions might have a different answer in the different countries. For example, how many years should Costeja data be available? What about crimes? Should we distinguish between different types of crimes? And what about the definition of 'public figure'?

It also affects the competition, since not every search engine has the resources, which Google has put into operation, to address the application of this ruling and manage the thousands of complicated requests they receive. As put by Leta Jones: "responding to user takedown requests is incredibly disruptive to operations of sites and services around the world-determination of validity, authentication, and country-specific legal interpretation of each claim will be so time-consuming, costly, and inconsistent that many will just remove content automatically. This conflicts with the European treatment of intermediaries."[288]

Professor Trudel has expressed concerns that the first beneficiaries of the RTBF may be the ones who wish to hide their past (and sometimes illicit) activities.[289] For instance, in the period that followed the Liberation of France, archives and other public documents that would have apparently been able to reveal some of the Collaboration's actions with the enemy were stolen. For Trudel, this illustrates the risks associated to a potentially abusive use of the RTBF. He also cautions against the fact that the RTBF would make it more difficult for social scientists or historians, who wish to understand certain social phenomenon or to report history, to use technology (i.e. the Internet) to do so.[290] He explains how we

[286] Article 29 Data Protection Working Party, "Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain", WP 179 Update (16 December 2015), online: <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2015/wp179_en_update.pdf>.

[287] Jones, *supra* note 271 at 173.

[288] *Ibid.* at 179.

[289] Pierre Trudel, "La menace du 'droit à l'oubli'", *Journal de Montréal* (11 April 2014), online: <http://www.journaldemontreal.com/2014/04/11/la-menace-du--droit-a-loubli>.

[290] *Ibid*.

cannot predict today what will be useful archives to historians in the coming decades. In that context, it is perhaps unsurprising that historians have expressed their concerns over the RTBF.[291]

RTBF supporters argue this will not be a concern because these claims will fail a balancing test. Although the bulk of requests in the EU have not been from criminals, politicians and public figures,[292] there certainly have been many requests from such individuals. Moreover, the adoption of the RTBF a legal right has begun to influence jurists to give greater right to those seeking to erase criminal convictions. For example, a few months after the *Google Spain* ruling, the Saitama district court of Japan relied on the RTBF in a case where a man demanded that Google remove reports posted online more than three years ago detailing his arrest and conviction for breaking child prostitution and pornography laws, for which he was fined 500,000 yen.[293] Japanese Courts, based on a right to privacy, have in the past often handled removal requests by plaintiffs. But here, referring for the first time to a concept of RTBF,[294] Presiding Judge Hisaki Kobayashi with the Saitama District Court granted removal of search results linking the man to reports of this terrible crime. The decision is on appeal.

Lila Tretikov, the executive director of Wikimedia Foundation, highlighted her censorship concerns of the ruling, stating that "accurate search results are vanishing in Europe with no public explanation, no real proof, no judicial review, and no appeals process." She added, "we find this type of veiled censorship unacceptable. But we find the lack of disclosure unforgivable. This is not a tenable future. We cannot build the sum of all human knowledge without the world's true source, based on pre-edited histories."[295]

3.2.3 Unequal Access to Data

Information is the main asset of the current digital era where we live and a powerful tool; that is why the access to information should be a fundamental right for all citizens, and not only for some of them. Making it difficult for certain citizens to access certain information, has the risk to place them in a disadvantaged situation. A RTBF in Canada would lead to unequal access to data. Canadians have easy access to and often use U.S. resources for research and information, and since the RTBF will never be acceptable in the U.S., as it will conflict with the First Amendment of the U.S. Constitution, any restriction on Canadian services will be ineffective. Even if Canadians are blocked from specific content on U.S. services, it would be trivial for them to bypass these blocks by using tools that make it appear they are using U.S. IP addresses, such as VPNs.

---

[291] Fabienne Dumontet, "Le 'droit à l'oubli numérique' inquiète les historiens", *Le Monde* (10 March 2013), online: <http://www.lemonde.fr/technologies/article/2013/10/03/le-droit-a-l-oubli-numerique-inquiete-les-historiens_3489513_651865.html#b25TsYJzuq6mbssI.99>.

[292] Sylvia Tippmann and Julia Powles, "Google accidentally reveals data on 'right to be forgotten' requests", *The Guardian* (14 July 2015), online: <https://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests>.

[293] Justin McCurry, "Japan recognises 'right to be forgotten 'of man convicted of child sex offences", *The Guardian* (1 March 2016), online: <http://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences>.

[294] KYODO, "Japanese court recognizes 'right to be forgotten' in suit against Google", *The Japan Times* (27 February 2016), online: <http://www.japantimes.co.jp/news/2016/02/27/national/crime-legal/japanese-court-recognizes-right-to-be-forgotten-in-suit-against-google/>.

[295] Alex Hern, "Wikipedia swears to fight 'censorship' of 'right to be forgotten' ruling", *The Guardian* (6 August 2014), online: <http://www.theguardian.com/technology/2014/aug/06/wikipedia-censorship-right-to-be-forgotten-ruling>.

3.3 Other Considerations and Practical Challenges

Finally, the introduction of a RTBF in Canada would raise other important concerns and would pose practical challenges. First, the constant evolution of social norms would lead to the erasure of certain information that was unacceptable at the time of the erasure, but that, over time, may gradually become acceptable or at least, less relevant (section 3.3.1). Second, the unequal implementation of a RTBF across different jurisdictions could ultimately lead to an extraterritorial application of the RTBF (section 3.3.2).

3.3.1 Evolving Social Norms

An aspect to consider before adopting an approach favouring the censorship of personal information online through a RTBF is the fact that perhaps, as a society, the norm of what is acceptable will evolve over time with the Internet and in light of the availability of the information. In other words, if more personal information is available online for longer periods of time, information pertaining to someone's distant past may be naturally considered as less and less relevant over time. Ambrose explains how like other resources, information is perishable, depreciating in value over time, and that depreciation will occur at different rates for different pieces of information, correlating to the content's relevance and accuracy.[296]

To illustrate this point further, in the fall of 2014, it was reported that Jacqueline Laurent-Auger, a Montreal theatre teacher at a private high school, was informed that her contract would not be renewed because she had appeared in several erotic films in the 1960s and early 1970s (while she was in her 20s), which students had found online, occasioning much distraction.[297] She had taught at the college for 15 years without incident. The public reacted very negatively to the school's decision, as many felt it was an unfair one, based on old and irrelevant facts, especially since the quality of her teaching was never in question. The school's administration, facing so much negative reaction on social media, had to issue a press release, and quickly revisit its decision, ultimately confirming that Laurent-Auger could be re-hired.[298] In another recent case, a Quebec TV show host was caught exposing himself in a park, for which he received a municipal infraction ticket.[299] The infraction became known and the public was divided on whether these activities were in fact matters of public interest.[300] He felt humiliated and quit his job, but then returned to being a TV host a few months later.[301] These cases

---

[296] Meg L. Ambrose, "A Digital Dark Age and the Right to Be Forgotten", 17:13 J. Internet L. 1 (2013) at 135 [Ambrose].

[297] Philippe Orfali, "Une prof de théâtre congédiée pour des scènes érotiques passées", *Le Devoir* (18 October 2014), online: Le Devoir <http://www.ledevoir.com/culture/actualites-culturelles/421471/une-prof-de-theatre-congediee-pour-des-scenes-erotiques-passees>.

[298] CBC News, "Jacqueline Laurent-Auger, teacher fired decades after erotic film roles, may be rehired", *CBC News* (22 October 2014), online: CBC News <http://www.cbc.ca/news/canada/montreal/jacqueline-laurent-auger-teacher-fired-decades-after-erotic-film-roles-may-be-rehired-1.2808539>; see also Philippe Orfali, "La prof de théâtre de nouveau la bienvenue à Brébeuf", *Le Devoir* (22 October 2014), online: Le Devoir <http://www.ledevoir.com/societe/education/421671/scenes-erotiques-la-professeure-suspendue-pourra-retourner-a-brebeuf-dit-la-direction>.

[299] John R. Kennedy, "Quebec star Joël Legendre admits lying about exposing himself", *Global News* (14 March 2015) online: Global News <http://globalnews.ca/news/1882760/quebec-star-joel-legendre-admits-lying-about-exposing-himself/>.

[300] Lise Ravary, "Joël Legendre et l'intérêt public", *Le Journal de Montréal* (14 March 2015) online: Le Journal de Montréal <http://www.journaldemontreal.com/2015/03/14/legendre-et-linteret-publique>.

[301] Hugo Dumas, "V recrute Joël Legendre", *La Presse* (16 July 2015), online: La Presse <http://www.lapresse.ca/arts/television/201507/16/01-4885931-v-recrute-joel-legendre.php>.

illustrate how the public and its attitudes must and will evolve with the information age.[302] For example, Ambrose mentions that more and more, we recognize that a teenager's partying Facebook photograph has little to do with her employability eight years later.[303]

Perhaps, one day, the interest of the public will not be related to information already available on the Internet (i.e. over time, everyone will have information about them available that they do not like), but instead, it will relate to information that individuals have censored, or that they are attempting to hide. For example, the website "Hidden from Google", launched by American web developer Afaq Tariq, archives deleted links, along with the relevant search term and the source that revealed the missing information.[304] It was reported that media stories involving a financial scandal, a shoplifter and a sexual predator have disappeared from Google search results only to reappear on the "Hidden from Google" webpage.[305] The British Broadcasting Corporation (BBC) now publishes the links to its stories that have been deleted from Google searches.[306] Some report how, since the RTBF was adopted in the EU in 2014, well over one hundred BBC stories have disappeared from Google searches – an alarming number if we consider that the stories may include newsworthy content, including stories about the sentencing of a rapist, the murder of an heiress and a court case defining what constitutes a game of football.[307] The website "Hidden from Google" and the BBC's publication of its delisted stories could arguably presage a "black market Google," a searching application that grows ever more popular, in proportion to the increase in the number of links deleted pursuant to the RTBF.[308]

3.3.2 Extraterritorial Reach of the RTBF

Finally, the RTBF entrains extraterritorial issues that should be considered. The applicability of the RTBF has been complex since the beginning. In a first approach, Google only delisted content considered inadequate or relevant from European extensions of its services (such as google.fr or google.de). However, the French data protection authority (*Commission Nationale de l'Informatique et des Libertés, CNIL*) among others stated that this measure was not enough for the effectiveness of the RTBF, since any user could easily switch to Google.com and access the full list of results.[309]

---

[302] Jessica Winter, *The Advantages of Amnesia*, *Boston Globe* (23 September 2007), online: Boston Globe <http://www.boston.com/news/globe/ideas/articles/2007/09/23/the_advantages_of_amne sia/?page=full>. ("People, particularly younger people, are going to come up with coping mechanisms. That's going to be the shift, not any intervention by a governmental or technological body."); See also Cunningham, "The Internationalization of Censorship", *supra* note 8 at 38.

[303] Ambrose, *supra* note 296 at 135.

[304] See *Hidden from Google*, <http://hiddenfromgoogle.afaqtariq.com/> (last visited August 14, 2015).

[305] See Jeff John Roberts, "'Hidden from Google' shows sites censored under EU's right-to be-forgotten law" *Gigaom* (16 July 2014), online: Gigaom <https://gigaom.com/2014/07/16/hidden-from-google-showssites-censored-under-eus-right-to-be-forgotten-law/>.

[306] Neel McIntosh, "List of BBC web pages which have been removed from Google's search results", *BBC Internet Blog* (25 June 2015), online: BBC <http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379>.

[307] *Ibid*.; see Jamie Condliffe, "BBC Is Listing Pages Removed By Google Under EU Right-To-Be-Forgotten", *Gizmodo* (29 June 2015, <http://gizmodo.com/bbc-is-listing-pagesremoved-by-google-under-eu-right-t-1714610528> discussed in Cunningham, "The Internationalization of Censorship", *supra* note 8 at 26.

[308] Cunningham, "The Internationalization of Censorship", *supra* note 8 at 26.

[309] Peter Sayer, "France tells Google to remove 'Right to be forgotten' search results worldwide", *PCWorld* (21 September 2015), online: <http://www.pcworld.com/article/2984524/privacy/france-rejects-googles-appeal-on-right-to-be-forgotten.html>.

In an effort to solve this problem, Google announced that it would use global positioning.[310] This measure would solve the aforementioned problem, since the content delisted would not be accessible to people physically based in European countries, even if they were using google.com. However, this solution entrained a paradox that the French authority[311] was not willing to accept which is that European citizens could access the full list of results, as soon as they were outside Europe. Hence, the CNIL rejected this approach saying that a person's right to privacy could not depend on the "geographic origin of those viewing the search results".[312] As a consequence, the French authority has fined Google 100,000 euros for not delisting results across all its websites. The CNIL considers that for the RTBF to be effective, it is necessary to delist the content considered inadequate or irrelevant across all Google websites, including Google's main site (Google.com), and this, regardless of the geographic location of those viewing the search results. The search engine announced that it would appeal the decision.

The CNIL's decision clearly overreaches its powers, since it tries to control the content viewed outside France and by everyone. According to this interpretation, countries applying the RTBF could decide the type of information or content accessible through search results by other countries, regardless of other rights or freedom of information that might exist in these other countries.

The challenges for such jurisdictional claims for Canada are obvious and, as a matter of fact, have already been brought before the courts. For instance, in *Equustek Solutions Inc. v. Google Inc.*,[313] the B.C. Court of Appeal dismissed Google's attempt to overturn an injunction that had an extraterritorial effect. In that case, Google had agreed to voluntarily de-index webpages from the Canadian version of their search site (Google.ca), but had refused to block the search results in other, non-Canadian versions of their site, including Google.com. In dismissing Google's argument that a more limited order should have been made, Justice Groberman wrote that: "[t]he plaintiffs have established, in my view, that an order limited to the google.ca search site would not be effective. I am satisfied that there was a basis, here, for giving the injunction worldwide effect."[314]

This decision, for which leave to appeal to the Supreme Court was granted on February 18, 2016,[315] raises concerns similar to those raised by the CNIL's decision. Indeed, this type of approach could lead to an increasing number of worldwide injunctions, or at least injunctions with a significant extraterritorial reach, against Internet search engines and other Internet-based companies. Individuals claiming listing and seeking a RTBF as envisioned by the CNIL or, at least to a certain extent, by the B.C. Court of Appeal would result in the claim that information must be deleted on U.S. services. Since the U.S. Courts are unlikely to be willing to accept the concept of a RTBF, the concept would create a challenging jurisdictional conflict. Given the linked economies of the two nations, with cross border employment and schooling, the likely legal disruption should be of concern. Finally, as mentioned by Robert G. Larson, such an extraterritorial effect not only allows someone from a different jurisdiction or country to

---

[310] Frederic Lardinois, "Google now uses geolocation to hide 'right to be forgotten' links from its search results", *Techcrunch* (4 March 2016), online: http://techcrunch.com/2016/03/04/google-now-uses-geolocation-to-hide-right-to-be-forgotten-links-from-its-search-results/>.

[311] *Commission Nationale de l'Informatique et des Libertés* (CNIL), online: <https://www.cnil.fr>.

[312] Julia Fioretti, "France fines Google over 'right to be forgotten'" *Reuters* (24 March 2016), online: <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX>.

[313] *Equustek*, *supra* note 53.

[314] *Ibid*.

[315] *Google Inc. v. Equustek Solutions Inc., et al.*, 2016 CanLII 7602 (SCC).

erase information that they perceive as "irrelevant" or "illegitimate" based on their own set of values; it also "subverts national sovereignty and arguably promotes one culture's value of individual privacy rights over other cultures' value of free expression."[316] Some countries with very different social or religious values could simply request to completely censor western content altogether.

[316] Robert G. Larson III, "Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten Are Incompatible with Free Speech" (2013) 18:91 *Comm. L. & Pol'y* 114 as reported in Cunningham, "The Internationalization of Censorship", *supra* note 8 at 6.

CONCLUSION

The CJEU's landmark ruling in the *Google Spain* case in 2014 has sparked a debate on the necessity of importing a RTBF in Canada. A RTBF would allow individuals to stop data controllers, such as Google, from providing links to information deemed irrelevant, no longer relevant, inadequate or excessive given the purpose for which it was processed and the time that has elapsed. While some ideas inherent in a RTBF may sound appealing at first blush, especially in view of the protection granted to the privacy of individuals and to their reputation, this paper articulates the view that importing this right into Canada would prove to be unconstitutional, unnecessary and inefficient, from both a legal perspective and a public policy perspective.

Section 1 illustrates the significant constitutional challenges associated with importing a RTBF in Canada and more specifically, that a European-style RTBF would fail to strike an appropriate balance between freedom of expression and privacy. A RTBF would infringe the constitutionally-protected right to freedom of expression of search providers, authors and webmasters, by hindering access to information in a way that would most likely not be demonstrably justified under section 1 of the Canadian Charter. Accordingly, any law purporting to create such a right would probably be struck down by Canadian courts.

Section 2 demonstrates that the current Canadian legal framework already contains several of the most appealing principles underlying the RTBF, which renders the latter unnecessary in Canada, at least in some jurisdiction such as Quebec. First, laws have been implemented to allow individuals to control their personal information, notably in the form of data protection statutes, as well as laws restricting the availability or use of information. Secondly, other pieces of legislation, such as privacy laws and enactments protecting reputation, efficiently restrict the dissemination of harmful personal information. In this respect, new legislative measures have been implemented, in combination with the recognition by courts of new privacy-related common law torts, to address new online privacy and reputational issues such as cyberbullying and "revenge porn". Thirdly, laws have been enacted in order to regulate web intermediaries and service providers, and to provide a certain level of protection against illicit information posted on the Internet, including defamation and other harm, while efficient takedown procedural tools are already in place in most jurisdictions to allow individuals to eradicate defamatory material online.

Finally, section 3 of this paper provides an overview of the practical reasons that make a RTBF impossible to implement without serious harms to a wide range of societal interests. The numerous and significant risks pertaining to the RTBF are related to entrusting private entities with the tasks of arbitrating fundamental rights and values, censorship, availability of historical information, and potential infringements on freedom of expression. Moreover, in light of the European experience over recent months, the RTBF has an extraterritorial reach that has important ramifications, including in the Canadian and broader North American context.

These constitutional, legal and public policy concerns all militate against importing a RTBF into Canada. This is not to say, however, that the complex legal framework currently in place in Canada perfectly addresses all of the privacy and reputational concerns the RTBF is meant to address. Indeed, it makes no doubt that certain provinces offer better protection against harmful or defamatory content than others. For instance, as mentioned in section 2, recovery for defamation in common law jurisdictions may be barred if the statements are true. In Québec, on the other hand, the accuracy of the information revealed to the public (or the fact that it is true) does not suffice to avoid civil liability. In that sense,

reputational rights are probably better protected in Québec than in other Canadian provinces, given that the personal information that is revealed to the public must not only be true or accurate; it must also be necessary to convey the particular content in which the public has a legitimate interest.

It is, however, unnecessary to import a RTBF to address such a concern and other similar concerns. First, it is possible for provincial legislatures to enact new laws or to adapt the existing legislation regarding privacy and defamation so as to cover new online phenomena, in the same way that they have done with respect to cyberbullying and “revenge porn”. Secondly, courts are already well-placed to strike an appropriate balance between the two fundamental values that are often opposed in similar situations, namely freedom of expression and privacy.

In that respect, it is important to bear in mind that the RTBF would be enforced by private corporations that have an incentive to err on the side of removal in order to reduce costs and/or to avoid legal liability and the hefty fines to which they are exposed in case of non-compliance. Courts, on the other hand, have the expertise and independence to properly balance fundamental rights and values. They, as public bodies, are in a much better position than private entities to act independently and justly to determine whether, and to what extent, the disclosure of any given personal information is in the public interest.

As mentioned earlier, the power to take down webpages or to remove hyperlinks is an important one, which should be taken seriously, given the possible adverse effects of such action on freedom of expression and the general availability of information. While there is still room for improvement, however, the current legal framework in Canada fosters the appropriate balance between freedom of expression and privacy, in light of the public interest. Efforts should now be directed to improving this legal framework, notably by increasing access to justice, rather than by an importing a RTBF that would very likely prove to be unconstitutional, unnecessary and counterproductive.