

DROIT À L'OUBLI: CANADIAN PERSPECTIVE ON THE GLOBAL 'RIGHT TO BE FORGOTTEN' DEBATE*

ELOÏSE GRATTON** AND JULES POLONETSKY***

European courts have recognized a “right to be forgotten” (RTBF) that would allow individuals to stop data search engines or other third parties from providing links to information about them deemed irrelevant, no longer relevant, inadequate, or excessive. There is a lack of consensus between the European Union and the United States on the legitimacy of this right, which illustrates the cultural transatlantic clash on the issue of the importance of privacy versus other rights, such as freedom of information and freedom of speech. This is problematic because privacy regulators in Europe have also pressed for a broad view of this right, seeking to extend it globally—requesting that information not only be delisted from European extensions, but from all extensions. Some are concerned that such an extraterritorial effect not only allows someone from a different jurisdiction or country to erase information that they perceive as “irrelevant” or “illegitimate” based on their own set of values; it also arguably promotes one culture’s value of individual privacy rights over other cultures’ value of free expression. While the Canadian Charter of Rights provides constitutional protection to fundamental freedoms such as freedom of expression, Canada has also adopted data protection laws, which are similar to the European Directive 95/46/EC.

This paper explores whether importing the RTBF would be legal in Canada. The authors argue that such a right may be

* We are grateful for the valuable contribution from attorneys Patrick Plante and 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. Their research for an earlier paper entitled: “Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada” submitted in April 2016 to the Privacy Commissioner of Canada, as part of its consultation on online reputation and privacy was extremely useful.

** Partner and National Co-Leader, Privacy and Data Security Practice Group of Borden Ladner Gervais LLP, Adjunct Professor, University of Montreal, Faculty of Law. 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.

*** CEO, Future of Privacy Forum, Adjunct Professor, Washington & Lee School of Law.

unconstitutional in Canada; it would most likely infringe upon freedom of expression in a way that cannot be demonstrably justified under the Canadian Constitution. The authors also argue that the legal framework in Quebec addresses some of the privacy and reputational concerns that a RTBF is meant to address through a “public interest” test, although they acknowledge that there are some limits to this framework. The notions of res judicata and periods of limitations must be revisited to ensure that this privacy framework can adequately address the fact that with the Internet, data can outlive the context in which they were published and considered legitimate. The fact that the data that was once considered outdated may become relevant again over time should also be considered. 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.

INTRODUCTION.....	339
I. RIGHT TO BE FORGOTTEN AND LEGAL RIGHTS AT STAKE	342
A. <i>Freedom of Expression and Information</i>	343
1. Freedom of Expression and of Information Concerns	343
a. <i>Over-Blocking Because of the RTBF</i>	343
b. <i>Right to History</i>	345
2. Legal Framework on Freedom of Expression	347
B. <i>Online Privacy and Reputation</i>	351
1. Legal Framework on Data Protection	352
2. Increased Availability of Information.....	355
a. <i>Spatial Shift</i>	356
b. <i>Temporal Shift</i>	357
II. CONSTITUTIONAL CHALLENGES WITH THE IMPLEMENTATION OF A RTBF	358
A. <i>Freedom of Expression as a Constitutional Right</i>	359
1. Court Intervention when Charter Rights Collide with Each Other: Oakes Test	359
2. The Scope of Freedom of Expression	361
B. <i>Can the RTBF be a Justified Limit to Freedom of Expression?</i>	365
1. Pressing and Substantial Objective.....	368
2. Rational Connection Between the Law and Its Objective	369
3. Minimum Impairment	369
4. Proportional Effect	374
III. IMPLEMENTATION OF A RTBF IN QUEBEC	377
A. <i>Challenges with the Implementation of a RTBF Under</i>	

<i>Quebec Law</i>	377
1. “Public Interest” Test.....	378
2. Courts Outsourcing the Balancing of Rights	383
B. <i>Limits to the Efficiency of Quebec Law</i>	386
1. <i>Res Judicata</i> and Prescription/Periods of Limitations	387
2. Decision on Retention and Restoring Data	388
CONCLUSION	389

INTRODUCTION

The Internet enables access to a vast range of knowledge, including a wide range of information about individuals around the world. Records document and allow the ownership of property, consumers to review service providers, and media researchers to describe events, large and small, which document the historical record. While access to information offers significant social benefits, it also carries risks to individuals. With Internet technologies, once published, a larger audience than before can access the information, and pieces of data can outlive the context in which they were initially published and considered legitimate. In response to these risks, European Courts have recognized a right to be forgotten (RTBF) and regulators have sought a wide interpretation of this right, which would provide individuals in European Union countries with a legal mechanism to compel the removal of their personal information from online searches.¹

The European Directive 95/46/EC already includes the principle underpinning the RTBF,² and the forthcoming General Data Protection Regulation (GDPR) specifically includes a “Right to Erasure.”³ The extent of this right was not established however,

1. While this right does not erase *per se* the original source of information, it will seek to hide information by removing results for queries that include certain names. An analogy would be a library removing book titles from their searchable catalogue. The actual books would remain on the shelves, but their existence would be unknown and therefore, their access made more difficult.

2. See EUROPEAN COMMISSION, FACTSHEET ON THE ‘RIGHT TO BE FORGOTTEN’ RULING (C-131/12), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf [hereinafter EUROPEAN COMMISSION FACTSHEET] [<https://perma.cc/BQ3R-UBGS>]. Support for the claim that the EU Directive includes the RTBF stems from Articles 6(1)(c) and 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, Nov. 23, 1995, 1995 O.J. (L 281) 31 [hereinafter Directive 95/46/EC].

3. *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 (General Data Protection Regulation)*, at 17, COM (2012) 11 final (Jan. 27, 2012) [hereinafter *GDPR*].

until the May 2014 landmark decision in *Google Inc. v. Agencia Española de Protección de Datos* (“Google Spain”).⁴ In this dispute, Spanish lawyer Mario Costeja González, after realizing that Google searches under his name linked him with an old news article pertaining to former debts, petitioned a Spanish court to order deletion of the record as to both the local newspaper, *La Vanguardia*’s publication and Google’s linking the same to Costeja,⁵ claiming that he had a right to be forgotten.⁶ The Spanish court referred the case to the Court of Justice of the European Union (CJEU) that held the auction publications could remain on the newspaper’s website, but mandated Google to delete any link connecting Costeja to them.⁷ As of the writing of this paper, Google has reported⁸ receiving over 466,370 requests takedown requests, covering over 1.5 million URLs.⁹

Lack of consensus exists as to whether such broad application of the RTBF to search engines is legitimate.¹⁰ Some warn that the standard to determine if the information should be removed (the information deemed “inadequate, irrelevant or no longer relevant, or excessive”) lacks objective guideposts.¹¹ Others welcome this new right, considering it as a way for individuals to better protect their online reputation.¹² This lack of consensus may illustrate, to a certain extent, the cultural transatlantic clash on the issue of the

4. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R.

5. *Id.* at ¶ 14.

6. *Id.*; see also Dave Lee, *What is the ‘Right To Be Forgotten?’*, BBC NEWS (May 13, 2014), <http://www.bbc.com/news/technology-27394751> [<https://perma.cc/2Q58-D2NB>].

7. *Google Spain SL*, 2014 E.C.R. at 18–20; see also EUROPEAN COMMISSION FACTSHEET, *supra* note 2.

8. See *Transparency Report: European Privacy Requests for Search Removals*, GOOGLE, <https://www.google.com/transparencyreport/removals/europeprivacy?hl=en-US> [<https://perma.cc/2D3G-M4EK>] (last updated Mar. 22, 2017).

9. Letter from Google to the Article 29 Working Party, Google (July 31, 2014), <https://docs.google.com/file/d/0B8syaai6SSfT0EwRUFyOENqR3M/edit?pli=1> [<https://perma.cc/KY5M-NCXA>] (Google confirmed removing hyperlinks in about 42% of such requests received.).

10. On February 24, 2017, the Conseil d’Etat requested the European Court of Justice for a preliminary ruling on a series of questions concerning the implementation of the right to be delisted. See *Right to be Delisted*, CONSEIL D’ÉTAT, (Feb. 24, 2017), <http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted> [<https://perma.cc/R632-8KHP>].

11. Robert Peston, *Why has Google Cast Me into Oblivion?*, BBC NEWS (July 2, 2014), <http://www.bbc.com/news/business-28130581> [<https://perma.cc/7D9E-4D4U>]; see also McKay Cunningham, *Free Expression, Privacy and Diminishing Sovereignty in the Information Age: The Internationalization of Censorship*, ARK. L. REV. 4 (forthcoming 2015); see also Jeffrey Toobin, *The Solace of Oblivion: In Europe, the Right to be Forgotten Trumps the Internet*, NEW YORKER (Sept. 29, 2014), <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion> [<https://perma.cc/7YDK-VRRW>].

12. Frank A. Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515 (2015); Paulan Korenhof & Ludo Gorzeman, *Who is Censoring Whom? An Enquiry into the Right to Be Forgotten and Censorship* (Working Paper, 2015), <http://dx.doi.org/10.2139/ssrn.2685105> [<https://perma.cc/TNZ7-2PDZ>].

importance of privacy versus other rights, such as freedom of information and freedom of speech.

Some commentators argue 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 8.¹³ 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, on the other side of the spectrum, have trust in the government and share a common distrust vis-à-vis the market.¹⁴

The lack of consensus on the legitimacy of the RTBF between jurisdictions presents problems because it entrains extraterritorial issues.¹⁵ Following the *Google Spain* decision, Google only delisted content from European extensions of its services such as google.fr or google.de. The French Data Protection Authority (*Commission Nationale de l'Informatique et des Libertés* or *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.¹⁶ In an effort to solve this problem, Google announced that it would use geo-blocking, making content delisted inaccessible to people physically based in European countries, even if they are using Google.com.¹⁷ CNIL rejected this solution on the basis that European citizens may still access the full list of results as soon as they are outside Europe, or by using tools that allow them to circumvent the geo-blocking.¹⁸ The challenge is 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

13. Franz Werro, *The Right to Inform v. The Right to be Forgotten: A Transatlantic Clash* 298 (Georgetown Public Law Research Paper No. 2, May 8, 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357 [<https://perma.cc/7HCL-NZYA>].

14. *Id.*

15. See David Hoffman, Paula Bruening, & Sophia Carter, *The Right to Obscurity: How We Can Implement the Google Spain Decision*, 17 N.C. J.L. & TECH. 437, 464–74 (2016) (the global impact of the implementation of Google Spain).

16. Peter Sayer, *France Tells Google to Remove 'Right to be Forgotten' Search Results Worldwide*, PCWORLD (Sept. 21, 2015, 7:00 AM), <http://www.pcworld.com/article/2984524/privacy/france-rejects-googles-appeal-on-right-to-be-forgotten.html> [<https://perma.cc/2S9Z-ZHGN>].

17. Frederic Lardinois, *Google Now Uses Geolocation to Hide 'Right to be Forgotten' Links From Its Search Results*, TECHCRUNCH (Mar. 4, 2016), <http://techcrunch.com/2016/03/04/google-now-uses-geolocation-to-hide-right-to-be-forgotten-links-from-its-search-results/> [<https://perma.cc/E9RN-VR6F>].

18. See Julia Fioretti, *France Fines Google Over 'Right to be Forgotten'*, REUTERS (Mar. 24, 2016, 3:10 PM), <http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX> [<https://perma.cc/9V28-ZXJX>].

other countries.¹⁹ As mentioned by Larson, such an extraterritorial effect not only allows someone from a different jurisdiction or country to 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.”²⁰

In Canada, the issue of freedom of expression and privacy has a balanced legal framework. While the Canadian Charter of Rights provides constitutional protection to fundamental freedoms such as freedom of expression, Canada has also adopted data protection laws that are similar to the European Directive 95/46/EC. Within Canada, Quebec, a primarily French-speaking province, has the most stringent privacy regime and reputational legal framework. Quebec could, in some ways, be considered as the “California” of Canada.²¹ Given Canada’s balanced legal framework on the conflicting issues at the heart of the RTBF, the following analysis may be of interest to some jurisdictions, especially those that believe that a global approach to addressing online privacy and reputation issues may be beneficial and easier to implement, or those looking to implement an efficient legal framework to address the issues at the heart of a RTBF.

Section 1 discusses two main rights, which the RTBF can either promote (online privacy and reputation) or constrain (freedom of expression and of information), as well as the Canadian legal framework protecting such rights. Section 2 discusses the constitutional challenges with the implementation of a RTBF in Canada. Section 3 elaborates on whether the RTBF can be easily implemented in Quebec, a province with a stringent privacy and reputation legal framework.

I. RIGHT TO BE FORGOTTEN AND LEGAL RIGHTS AT STAKE

While the RTBF may be considered a privacy and reputation-enhancing tool, there are reasons that make a RTBF challenging to implement without serious harm to a wide range of societal interests and rights. The fundamental right of freedom of

19. This type of jurisdictional challenge has already been brought before the Canadian courts in *Equustek Solutions Inc. v. Google Inc.*, [2015] B.C.C.A. 265 (Can.). 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. This case is under appeal and was heard by the Supreme Court of Canada on December 6, 2016 (and is presently awaiting judgment).

20. Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten Are Incompatible with Free Speech*, 18 COMM. L. & POL’Y 91, 114 (2013).

21. In Quebec, the legal framework is generally more protective of consumers and the privacy legal framework is more stringent than in the rest of Canada.

expression could be affected, as well as the right to access of information. Privacy and freedom of expression are both protected in Canada, a jurisdiction which can be viewed as one which shares similarities with both the United States and the EU legal framework on the rights which are at stake with the RTBF: privacy, freedom of expression, and freedom of information.

A. Freedom of Expression and Information

One of the most repeated arguments against a RTBF is that it would constitute a concealed form of censorship.²² As Jef 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 defamation and privacy laws around the globe are already massively abused to censor legitimate speech. The introduction of a 'right to be forgotten' [sic] arguably, adds yet another censoring opportunity.²³

The EU and Canada approach the protection of freedom of expression similarly, while the United States and the Canadian Supreme Courts share the same approach in managing freedom of expression cases.

1. Freedom of Expression and of Information Concerns

The consequences of the censoring opportunity triggered by a RTBF are twofold. From a data controller's (i.e., a search engine) standpoint, compliance with a RTBF may prove burdensome in practice.²⁴ As a consequence, a RTBF could have a chilling effect on service providers that might want to avoid liability by over-blocking content. The introduction of a RTBF could also have a negative impact on the availability of important material online, including historical material.

a. Over-Blocking Because of the RTBF

Search engines and web intermediaries are usually not

22. Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, (Mar. 9, 2011), <http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html> [<https://perma.cc/Q24Q-UXC8>].

23. Jef Ausloos, *The 'Right to Be Forgotten' – Worth Remembering?*, 28 COMPUT. L. & SEC. REV. 143 (2012).

24. MEG LETA JONES, CTRL+Z: THE RIGHT TO BE FORGOTTEN 179 (N.Y.U. Press, 2016).

responsible for content published or made available online.²⁵ 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. 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.”²⁶ Rosen says that because the tech companies cannot know in advance whether a particular request is will be granted, they will 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 an arbiter of what information is relevant or damaging.²⁷ Although Google apparently devoted tremendous resources to its review process, buttressed by a clear corporate commitment to maximum support for free speech seeking to maintain relevant content,²⁸ few will risk the liability when faced with potential fines and penalties for not removing such content immediately upon objection by users. Not every search engine can manage the thousands of complicated requests they receive due to limited resources.²⁹

Those who support a RTBF sometimes argue that companies have been able to comply with copyright law that requires a notice and takedown-type procedure in the United States.³⁰ Indeed this comparison to copyright is worth further scrutiny. The United States and Canadian 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

25. In Quebec, see the Act to Establish a Legal Framework for Information Technology, c C-1.1, s. 22. In the U.S., see 47 U.S.C. § 230 (2012).

26. Marc Gollom, *Google Looms as ‘Censor-in-Chief’ After ‘Right to be Forgotten’ Ruling*, CBC NEWS (May 14, 2014, 5:00 AM), <http://www.cbc.ca/news/world/google-looms-as-censor-in-chief-after-right-to-be-forgotten-ruling-1.2641714> [<https://perma.cc/7LJX-XDGM>].

27. *Should We Have the ‘Right to be Forgotten’ Online?*, WNYC (May 13, 2014), <http://www.wnyc.org/story/should-we-have-right-be-forgotten-online/> [<https://perma.cc/Q5XB-UY5F>].

28. *The Advisory Council to Google on the Right to be Forgotten*, GOOGLE, <https://www.google.com/advisorycouncil/> [<https://perma.cc/Y2GS-9RQ7>] (last visited Mar. 22, 2017) (Google created a special committee to analyze RTBF removal requests).

29. As put by Meg Leta Jones: “[r]esponding 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.” JONES, *supra* note 24, at 179.

30. Toobin, *supra* note 11.

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 web publishers take-down notices to object to content they claim is unlawfully posted. The assessment of whether a particular posting is protected by fair use is often complex and there is a significant grey area in which fair use may or may not apply.³¹ As organizations face liability if uncooperative or inaccurate, fair use advocates believe that companies prefer to avoid liability and quickly take down legal content.³² The concerns of the fair use advocates provide serious caution for a system that would similarly have a search engine having to make a choice between liabilities and defending inclusion of search results.

b. Right to History

Tim John Berners-Lee, the creator of the World Wide Web, has stated that, at present, the introduction of a RTBF is dangerous, as it can undermine the right to freedom of expression and freedom of information, but also the right to history.³³ 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.³⁴ Likewise, Jimmy Wales, founder of Wikipedia has spoken out on different occasions against the controversial *Google Spain* decision, describing the RTBF as “deeply immoral.”³⁵ In his opinion, history is a human right and one of the worst transgressions is to attempt to force silence on another or try to suppress the truth.³⁶ Since the *Google Spain* decision, Wikimedia Foundation has received multiple notices of intent to remove Wikipedia content from European search results and has decided

31. RICHARD STIM, *GETTING PERMISSION* (NOLO, 5th ed. 2013).

32. Paul Sieminski, *Corporations Abusing Copyright Laws are Ruining the Web for Everyone*, WIRED (May, 17 2014, 9:35 AM), <http://www.wired.com/2014/01/internet-companies-care-fair-use/> [<https://perma.cc/S29L-HWQT>] (“This 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.”).

33. Stephen Shankland, *Web Founder: Europe’s Right to be Forgotten Rule is Dangerous*, CNET (Dec. 10, 2014, 4:03 AM), <http://www.cnet.com/news/web-founder-europes-right-to-be-forgotten-rule-is-dangerous/> [<https://perma.cc/G9MS-2UZ6>] (“This right to be forgotten—at the moment, it seems to be dangerous.”).

34. Agence France-Presse, *Tim Berners-Lee Calls for Internet Bill of Rights to Ensure Greater Privacy*, GUARDIAN (Sept. 27, 2014, 11:26 PM), <https://www.theguardian.com/technology/2014/sep/28/tim-berners-lee-internet-bill-of-rights-greater-privacy> [<https://perma.cc/GU4W-2LB4>] (articulating the view that the problem of information available online for a long period should be addressed from another perspective, perhaps by implementing rules that protect people from the inappropriate use of old information).

35. Sophie Curtis & Alice Philipson, *Wikipedia Founder: EU’s Right to be Forgotten is ‘Deeply Immoral’*, TELEGRAPH (Aug. 6, 2014, 12:07 PM), <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html> [<https://perma.cc/8TD9-W7N9>].

36. *Id.*

to release a list of these notices received from search engines in one of their pages.³⁷

Lila Tretikov, the Executive Director of Wikimedia Foundation, highlighted her censorship concerns of the ruling, stating “accurate search results are vanishing in Europe with no public explanation, no real proof, no judicial review, and no appeals process.”³⁸ She added, “[w]e 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.”³⁹

Professor Trudel has also expressed concerns that the first beneficiaries of the RTBF may be the ones who wish to hide the past (and sometimes illicit) activities.⁴⁰ 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.⁴¹ More specifically, a substantial number of documents were stolen and destroyed due to their highly compromising nature.⁴² During the liberation, agents of the Investigation and Enforcement Unit (*Section d’enquête et de contrôle*), which had taken some of the responsibilities and duties of the Jewish Issues Police (*Police aux questions juives*), burned a significant amount of sensitive and compromising documents in an attempt to delete traces of the horrendous acts committed against the Jewish population of France.⁴³ For Trudel, this illustrates the risks associated with a potentially abusive use of the RTBF. He also cautions against the fact that the RTBF would make it more difficult for social scientists

37. *Notices Received from Search Engines*, WIKIMEDIA FOUND., https://wikimediafoundation.org/wiki/Notices_received_from_search_engines [https://perma.cc/UTR9-NKD2] (last visited Mar. 23, 2017).

38. Curtis & Philipson, *supra* note 35.

39. Alex Hern, *Wikipedia Swears to Fight ‘Censorship’ of ‘Right to be Forgotten’ Ruling*, GUARDIAN (Aug. 6, 2014, 8:04 AM), <http://www.theguardian.com/technology/2014/aug/06/wikipedia-censorship-right-to-be-forgotten-ruling> [https://perma.cc/TG3J-42U3].

40. Pierre Trudel, *La menace du ‘droit à l’oubli’*, J. MONTRÉAL (Apr. 11, 2014, 6:00 PM), <http://www.journaldemontreal.com/2014/04/11/la-menace-du-droit-a-loubli> [https://perma.cc/8ZVZ-2X7T]; see Justin McCurry, *Japan Recognizes ‘Right to be Forgotten’ of Man Convicted of Child Sex Offences*, GUARDIAN (Mar. 1, 2016, 5:16 PM), <http://www.theguardian.com/technology/2016/mar/01/japan-recognises-right-to-be-forgotten-of-man-convicted-of-child-sex-offences> [https://perma.cc/5C84-GJMA] (recognizing a RTBF in Europe has also begun to influence jurists in foreign jurisdictions to give greater right to those seeking to erase criminal convictions).

41. *Id.*

42. Caroline Piketty, Christophe Dubois & Fabrice Launay, *Guide de Recherché dans les Archives des Spoliations et des Restitutions: Mission D’étude sur la Spoliation des Juifs de France* 15 (2000), <http://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/014000425.pdf> [https://perma.cc/MBS2-RH8D].

43. *Id.* at 15–16.

or historians, who wish to understand certain social phenomenon or to report history, to use the Internet as a tool to do so.⁴⁴ He explains that we cannot predict today what will be useful as an archive to historians in the coming decades.⁴⁵ In this context, it is unsurprising that historians have expressed their concerns over the RTBF.⁴⁶

2. Legal Framework on Freedom of Expression

The constitutional entrenchment of civil liberties occurred recently in Canadian history. Originally, when the 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 concept of including a bill of rights.⁴⁷ Until the end of the 20th century, the protection of rights and freedoms was left to the common law and to ordinary statutes.⁴⁸ Given that these ordinary statutes were subject to parliamentary sovereignty, little judicial oversight existed at the time.⁴⁹ Judicial review was, in most respects, limited to legal issues regarding division of powers. The approach changed in 1982 with the enactment of the Canadian Charter of Rights and Freedoms (the “Charter”),⁵⁰ the Canadian counterpart of the American Bill of Rights.

As part of the formal Constitution of Canada, the Charter can only be changed through complex—and politically sensitive—amendment procedures, thus ensuring that guaranteed rights and freedoms will not be abrogated by ordinary legislative action.⁵¹ The Charter applies to all levels of government, but not directly to private activity.⁵² Due to its supreme status, it overrides any

44. *Id.*

45. Trudel, *supra* note 40.

46. Fabienne Dumontet, *Le ‘Droit à l’oubli Numérique’ Inquiète les Historiens*, MONDE (Mar. 10, 2013), http://www.lemonde.fr/technologies/article/2013/10/03/le-droit-a-l-oubli-numerique-inquiete-les-historiens_3489513_651865.html#b25TsYJzuq6mbssI [<https://perma.cc/UN7H-LDS5>].

47. *See* Constitution Act, 1867, 30 & 31 Vict, c 3 (U.K.), *reprinted in* R.S.C. 1985, app II, no 5 (Can.).

48. Ordinary statutes that protect civil liberties include the Canadian Bill of Rights, SC 1960, c 44 (Can.), which was adopted in 1960 with little effect. *See* PETER W. HOGG, CONSTITUTIONAL LAW OF CANADA 35-10 to 11 (Carswell, 5th ed. 2007).

49. *Id.* at 1-6, 34-2 to 36-2. (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.)

50. The Canada Act 1982 is the British statute which put an end to the authority of the United Kingdom Parliament over Canada. *See* Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act, 1982, c 11 (U.K.) [hereinafter Charter].

51. *Id.* § 52(3).

52. *Id.* § 32; *see* HOGG, *supra* note 48, at 37-18 to -19 (There is still ample debate and confusion about the reach of the Charter, especially with respect to government

inconsistent federal or provincial law, effectively providing a basis for judicial review of legislation and regulations, which curtail civil liberties.⁵³ 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,⁵⁴ 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.⁵⁵

At first blush, the Canadian protection granted to freedom of speech appears to be closer, in many respects, to the European approach to constitutionally protected rights than to the American approach. Indeed, the Canadian approach to fundamental rights seems more closely aligned with what Professor Kai Möller has dubbed the “global model” of constitutional rights.⁵⁶ This “global model” is the approach that has been adopted by several constitutional courts across the world since the end of the Second World War, most notably the European Court of Human Rights (ECtHR), the German Federal Constitutional Court (*Bundesverfassungsgericht*), the Constitutional Court of South Africa and, more recently, the United Kingdom House of Lords (now the Supreme Court).⁵⁷ This model is characterized by an extremely broad and inclusive approach to the scope of rights protected by the Constitution, as well as by the use of the doctrines of balancing and proportionality to determine the permissible limitations of rights.⁵⁸ The model primarily features a “proportionality test.” While there are different variations, it usually involves a balancing exercise wherein a fundamental or constitutionally protected right can be balanced against a competing right or public interest.⁵⁹ For instance, the ECtHR developed a proportionality test wherein a breach of a fundamental right can be acceptable if the impugned policy furthers a legitimate aim, answers a pressing social need, and if the measure is proportionate to the achievement of the legitimate aim pursued.⁶⁰ In the United States, the freedom of

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.).

53. See HOGG, *supra* note 48, 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).

54. See Charter, *supra* note 50, at § 2(b).

55. “Principles of fundamental justice” replaces the notion of “due process” found in the American Fifth Amendment. See U.S. CONST. amend V.

56. See KAI MÖLLER, *THE GLOBAL MODEL OF CONSTITUTIONAL RIGHTS 2* (Oxford Univ. Press, 2012).

57. *Id.*

58. *Id.* at 23.

59. *Id.* at 13.

60. See *Norris v. Ireland* (1991) 13 E.H.R.R. 186, ¶ 41.

speech is protected by the First Amendment of the United States Constitution, federal law, and several state constitutions and pieces of legislation. By contrast, the United States Supreme Court has developed over the years a drastically different approach to fundamental rights. First, the scope of rights protected by the United States Constitution is much smaller than in Europe and other jurisdictions that have adopted the “global model.” The United States Supreme Court only recognizes a “liberty interest” as a right insofar as it is “deeply rooted in this Nation’s history and tradition.”⁶¹ Justice Rehnquist explained this judicial restraint or caution in *Washington v. Glucksberg*, stating “[b]y extending constitutional protection to an asserted right or liberty interest, we, to a great extent, place the matter outside the arena of public debate and legislative action. We must therefore ‘exercise the utmost care whenever we are asked to break new ground in this field.’”⁶² Second, the United States Supreme Court has not adopted, contrary to most courts under the “global model,” a proportionality test to determine the permissible limitations of rights. Instead, United States constitutional law uses different standards, most notably the stringent strict scrutiny test, which “demands that a law interfering with a fundamental right must serve a compelling government interest and be narrowly tailored to the achievement of that interest.”⁶³ This standard of review has been qualified by certain scholars as “‘strict’ in theory and fatal in fact,”⁶⁴ with the popular perception that most laws fail when subjected to this standard.⁶⁵

Given the broad scope of rights protected by the Canadian Charter and the proportionality test developed by the Supreme Court of Canada in *R. v. Oakes*, which has become widely known as the “*Oakes Test*,”⁶⁶ it leaves no doubt that the Canadian approach to fundamental rights is more in line with the global (or European) model than the American model. Yet, despite these resemblances, it appears that, with regards to freedom of speech specifically, the Canadian protection granted to that right is substantially similar to the American one.

For instance, both the United States and the Canadian Supreme Courts appear to share the same approach—notably that

61. See, e.g., *Washington v. Glucksberg*, 521 U.S. 702 (1997); see generally, MÖLLER, *supra* note 56, at 17.

62. *Glucksberg*, 521 U.S. at 720.

63. MÖLLER, *supra* note 56, at 18.

64. See, e.g., Gerald Gunther, *The Supreme Court, 1971 Term—Foreword: In Search of Evolving Doctrine on a Changing Court: A Model for a Newer Equal Protection*, 86 HARV. L. REV. 1, 8 (1972).

65. *But see*, Adam Winkler, *Fatal in Theory and Strict in Fact: An Empirical Analysis of Strict Scrutiny in the Federal Courts*, 59 VAND. L. REV. 793 (2006) (for a critical assessment of this perception).

66. See *infra* Section 1 (discussing the *Oakes* test).

inaccurate, false, or erroneous statements should be protected by the freedom of speech—and seem equally in favor of a more free “marketplace of ideas,” according to which the truth will emerge from the competition of ideas in free, transparent public discourse.⁶⁷ This common American/Canadian approach is to be contrasted with the European approach whereby untrue facts are not protected by the Constitution. For instance, in its famous *Auschwitzlüge* (‘Auschwitz lie’) decision,⁶⁸ the German Constitutional Court held that denial of Holocaust is not protected by freedom of expression, given the large amount of evidence that this historical event happened. The Court interestingly draws a distinction between opinions and facts: if opinions will always be protected, the protection of “facts” will depend on whether they are true or untrue. In the Court’s view, facts are often necessary to form opinions, therefore they are also protected. However, if they are untrue, they cannot contribute in any meaningful way to the discussion. Therefore, if facts are untrue, they cannot be protected.

In a landmark case issued in 1967, *Time, Inc. v. Hill*,⁶⁹ the United States Supreme Court balanced the issue of privacy with the principle of freedom of speech protected under the First Amendment to the United States Constitution.⁷⁰ In this case, an author wrote a fictitious novel—later adapted into a play—loosely based on a real-life hostage taking in a private home that occurred in 1952. After a magazine published an account of the play and related it to the hostage-taking incident by describing the play as a re-enactment of the incident, the victim of the 1952 hostage taking sued the magazine. He argued that the article gave the knowingly false impression that the play depicted the 1952 hostage-taking incident. The Supreme Court decided in favor of the magazine and notoriously held that “erroneous statements about a matter of public interest . . . are inevitable, and, if innocent or merely negligent, must be protected if ‘freedoms of expression are to have the breathing space’ that they ‘need to survive.’”⁷¹ The *Hill* case thus made it difficult to recover against the press for the publication of non-defamatory facts. It must be emphasized, however, that inaccurate, false, or erroneous facts -already benefited from a certain level of constitutional protection, even before the *Hill* case was rendered. For instance, in an earlier case, *New York Times Co. v. Sullivan*,⁷² the Supreme Court had notably held that, as applied

67. It is worth mentioning, however, that Justices Cory and Iacobucci, in their dissenting opinion in *R. v. Zundel*, [1992] 2 S.C.R. 731 (Can.) expressly rejected this notion as an “inadequate model.”

68. BVerfGE 90, 241–55 (Apr. 13, 1994).

69. *Time, Inc. v. Hill*, 385 U.S. 374 (1967).

70. *See id.*

71. *See id.*

72. *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964).

to public figures, actual error, content defamatory of official reputation, or both, are insufficient for an award of damages for false statements unless actual malice—knowledge that the statements are false or in reckless disregard of the truth—is alleged and proved.⁷³

In Canada, the Supreme Court had a similar approach in *R. v. Zundel*.⁷⁴ In that case, a man had been charged for “spreading false news” under Section 181 of Canadian Criminal Code after publishing a pamphlet suggesting that the Holocaust was a myth perpetrated by a Jewish conspiracy.⁷⁵ The Supreme Court struck down this provision of the *Criminal Code* on the basis that it violated freedom of expression as protected under Section 2(b) of the Canadian Charter. Writing for the majority, Justice McLachlin noted that the wording of the provision was vague and broad, extending the scope of the provision to “virtually all controversial statements of apparent fact which might be argued to be false and likely to do some mischief to some public interest.”⁷⁶ Moreover, Justice McLachlin noted that the criminal nature of the provision created a real danger of a “chilling effect on minority groups or individuals, restraining them from saying what they would like for fear that they might be prosecuted.”⁷⁷

In light of the constitutional protection granted to inaccurate, false, or erroneous statements, and to freedom of speech in general, United States and Canadian constitutional law appear to share the same approach vis-à-vis the protection granted to fundamental rights.

B. Online Privacy and Reputation

The rights to privacy and reputation are usually protected in Europe and North America, although the scope of protection will vary depending on the jurisdiction. The Canadian Charter gives constitutional protection to, *inter alia*, the right to be secure against unreasonable search or seizure, at Section 8.⁷⁸ The Charter does not specifically protect the right to privacy, in contrast to the Charter of Fundamental Rights of the European Union⁷⁹ and the European Convention on Human Rights.⁸⁰ Nonetheless, as is the case with

73. *Id.*

74. *R. v. Zundel*, [1992] 2 S.C.R. 731 (Can.).

75. Canadian Criminal Code, R.S.C. 1985, c C-46.

76. *R. v. Zundel*, 2 S.C.R. at 731.

77. *Id.*

78. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c 11, s. 8 (U.K.).

79. Charter of Fundamental Rights of the European Union, 2007 O.J. (C 303).

80. COUNCIL OF EUROPE, CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS, E.T.S. NO. 5, 4 art. 8 (1950).

the United States Constitution,⁸¹ Canadian courts have inferred from the legal rights declared in the Charter a limited right to a reasonable expectation of privacy, especially from state intrusion,⁸² and have recognized privacy as a “fundamental value that lies at the heart of a democracy”.⁸³

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 this information is accessed and used.⁸⁴ Data protection laws (“DPLs”) generally include a right allowing individuals to control their personal information, and they are usually the laws most readily associated with the RTBF, although these laws have some limits when addressing some of the online privacy concerns that are at the core of a RTBF.

1. Legal Framework on Data Protection

The privacy threats resulting from the growing number of automated data banks and computers led to conceptualizing privacy as the “control over personal information” in the early 1970s.⁸⁵ This concept of “control” also led to the well-known international standard for data protection: the Fair Information Practices (FIPs), which is at the core of DPLs and the foundation for most DPLs around the globe, until today.⁸⁶

In Europe the FIPs were first incorporated in Convention 108.⁸⁷ At the end of the 1980s, it became clear in Europe that Convention 108 could not be used as a harmonizing tool across European states adopting DPLs, as the ones that had adopted such

81. McKay Cunningham, *Diminishing Sovereignty: How European Privacy Law Became International Norm*, 11 SANTA CLARA J. INT’L L. 421, 443 (2013).

82. More specifically, a limited right to privacy has been found to derive from Section 7 (“life, liberty and security”) and Section 8 (protection against “unreasonable search and seizure”) of the Charter. *See, e.g., Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, ¶ 25 (Can.); *R. v. O’Connor*, [1995] 4 S.C.R. 411, ¶¶ 110–119 (Can.) (J. L’Heureux-Dubé, concurring); *see also* MICHAEL POWER, *THE LAW OF PRIVACY* 231–252 (2013).

83. UFCW, *Local 401 v. Alta. (Info. and Privacy Comm’r)*, [2013] 3 S.C.R. 733, ¶ 19 (Can.).

84. POLICY AND RESEARCH GROUP OF THE OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, *ONLINE REPUTATION: WHAT ARE THEY SAYING ABOUT ME?* 13 (2016), <http://go.utlib.ca/cat/10616705> [<https://perma.cc/8MV5-NUB4>] [hereinafter *ONLINE REPUTATION*].

85. ELOISE GRATTON, *UNDERSTANDING PERSONAL INFORMATION: MANAGING PRIVACY RISKS* 6 (LexisNexis Canada, 2013).

86. *Id.* The OECD set out these principles. OCED, *THE OECD PRIVACY FRAMEWORK* (2013), http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [<https://perma.cc/E8GR-WNQF>]. In Canada, they were further developed by the Canadian Standards Association in its Model Code for the Protection of Person Information, CANADIAN STANDARDS ASSOCIATION, *MODEL CODE FOR THE PROTECTION OF PERSONAL INFORMATION* (CSA Publications, 1996), and adopted in the Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c 5.

87. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. 108.

laws had substantial differences.⁸⁸ This created problems in the European internal market and has led to the adoption of Directive 95/46/EC at the European level.⁸⁹ The Directive was meant to protect the fundamental rights and freedoms of natural persons, in particular their right to privacy with respect to the processing of personal data.⁹⁰ The European Commission put forward its EU Data Protection Reform in January 2012 to make Europe fit for the digital age. The upcoming GDPR is based on the FIPs and also includes a Right to Erasure, which can be assimilated to a RTBF.⁹¹

In North America, while the conception of “privacy as control over personal information” has been adopted by Canadian courts⁹² as well as United States courts,⁹³ Canada has adopted general DPLs that regulate the processing of all personal information. Meanwhile in the United States, privacy is protected by a patchwork of laws at the state and federal levels, which usually focus on protecting certain types of more sensitive information.

The Privacy Act of 1980 marked Canada’s first attempt to legislate in the area of data protection; however, it only covered the public sector.⁹⁴ With the rapid advances in information technology and the pressure to conform to European standards to facilitate cross-continental trade, new legislation was soon required. The federal Parliament and provincial legislatures alike have since then enacted data protection laws in both the public and private sector.⁹⁵

88. COLIN J. BENNETT & CHARLES D. RAAB, *THE GOVERNANCE OF PRIVACY* 93 (MIT Press, 2006).

89. *Id.*

90. *See* Council Directive 95/46, preamble, 1995 O.J. (L 281) 31 (EC) [hereinafter Council Directive 95/46].

91. Council Regulation 2016/679, 2016 O.J. (L 119) 1 (EU).

92. The conception of privacy as “control over personal information” has been adopted by the Supreme Court of Canada on several occasions. *See, e.g.*, *R v. Tessling*, [2004] 3 S.C.R. 432, ¶ 23 (Can.); *R. v. Edwards*, [1996] 1 S.C.R. 128, ¶ 61 (Can.); *R. v. Dymont*, [1998] 2 S.C.R. 417, ¶¶ 17, 20 (Can.).

93. The United States Supreme Court echoes this conception by stating that privacy “encompass[es] the individual’s control of information concerning his or her person.” *See* *United States DOJ v. Reporters Comm. for Freedom of the Press*, 489 U.S. 749, 763 (1989).

94. Privacy Act, R.S.C. 1985, c P-21.

95. In terms of constitutional distribution of powers, under the Canadian constitution, the provincial governments are given exclusive jurisdiction over matters of property and civil rights in each province. *See* David Fraser, *You’d Better Forget the Right to be Forgotten in Canada*, CANADIAN PRIVACY L. BLOG (Apr. 28, 2016, 3:29 PM), <http://blog.privacylawyer.ca/2016/04/you-d-better-forget-right-to-be.html> [<https://perma.cc/FU3Q-FHLE>]. Privacy is a matter of civil rights, as is non-criminal law that would mandate the removal of content such as that referred to by the complainant.

The federal government bases PIPEDA on the “General Trade and Commerce Power” that is located within s. 91(2) of the Constitution Act, 1867. To be valid federal legislation rooted in the general branch of the trade and commerce clause, the law would have to follow the indicia set out in *General Motors of Canada Ltd. v. City National Leasing*, [1989] 1 S.C.R. 641, ¶ 133 (Can.); *see also* MICHAEL POWER, *THE LAW OF PRIVACY* 11–12 (LexisNexis Canada, 2013) (according to Power, federal and provincial governments have concurrent jurisdiction in matters of privacy).

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.⁹⁶

At the Canadian federal level, the Personal Information Protection and Electronic Documents Act (PIPEDA) was introduced in 2000 and came into force in the private sector in 2004.⁹⁷ The federal government may exempt organizations or activities in Canadian provinces that have their own DPLs if they are substantially similar to PIPEDA.⁹⁸ The provinces of British Columbia, Alberta, and Quebec have enacted provincial DPLs that have been recognized as substantially similar to PIPEDA.⁹⁹ Under the Directive 95/46/EC, strict conditions apply to personal data transfers to countries outside the European Economic Area that are not considered to provide an adequate level of data protection.¹⁰⁰ The European Commission declared PIPEDA “adequate” in 2001.¹⁰¹ Canadian DPLs can therefore be considered as providing a privacy protection similar to those under the Directive 95/46/EC.

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,’”¹⁰² implying that this right already exists and is simply in need of reinforcement.¹⁰³ PIPEDA and substantially similar provincial laws, already include, to a certain extent, the principle underpinning the RTBF. The RTBF can more or less be reflected through the current obligations in DPL to obtain consent when using or disclosing personal information, to delete personal information when no longer relevant or inaccurate, and through the data minimization principle—prohibiting an organization from collecting, using or

96. *Lavigne v. Canada (Office of the Commissioner of Official Languages)*, [2002] 2 S.C.R. 53, ¶¶ 24–26 (Can.); *UFCW, Local 401 v. Alta. (Info. and Privacy Comm’r)*, [2013] 3 S.C.R. 733, ¶ 19 (Can.).

97. PIPEDA, S.C. 2000, c 5, s. 3 (Can.).

98. Under paragraph 26(2)(b) of PIPEDA, the Governor in Council can exempt an organization, a class of organizations, an activity, or a class of activities from the application of PIPEDA with respect to the collection, use or disclosure of personal information that occurs within a province that has passed legislation deemed to be substantially similar to the PIPEDA. *Id.*

99. *An Act Respecting the Protection of Personal Information in the Private Sector*, R.S.Q. 1993, c P-39.1 (Can.); *Personal Information Protection Act*, S.A. 2003, c P-6.5 (Can.); *Personal Information Protection Act*, S.B.C. 2003, c 63 (Can.).

100. Council Directive 95/46, *supra* note 90, at art. 25(6).

101. Commission Decision 2002/2, 2002 O.J. (L 2) 13 (EC); *but see* Gabe Maldoff & Omar Tene, ‘Essential Equivalence’ and European Adequacy After Schrems: *The Canadian Example*, WIS. INT’L L. J. (forthcoming Jan. 2017) (Some authors have raised the question that perhaps the adequacy assessment for Canada should be revisited.).

102. Viviane Reding, *The Upcoming Data Protection Reform for the European Union*, 1 INT’L DATA PRIV. L. 3, 4 (2011).

103. Bert-Jaap Koops, *Forgetting Footprints, Shunning Shadows: A Critical Analysis of the ‘Right to Be Forgotten’ in Big Data Practice*, 8 SCRIPTED 229, 233–34 (2011).

disclosing more personal information than necessary for the purpose identified.¹⁰⁴ While DPLs could be considered as already catering to a RTBF, through such rights and principles, these rights are not identical to the RTBF.¹⁰⁵ The RTBF affects search engines; the DPL rights place responsibility on the organization that collects and processes the information in the first place (i.e. online publishers or webmasters).

DPLs also 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.¹⁰⁶ Moreover, DPLs are based on a 40-year-old standard, FIPs, which provides that individuals should be in control of their personal information, although the Internet and related technologies are challenging this concept of privacy.

2. Increased Availability of Information

When the FIPs were first elaborated in Europe in the 1970s, reports on data protection were assessing whether to draw a distinction between what they called “public” and “private” information (the former class, including matters such as data subject’s name, address, and sometimes age and marital status).¹⁰⁷ Some regulators did not believe that the simple distinction between “public” versus “private” information was feasible, or that it would be useful if it could be made.¹⁰⁸ Some also questioned the relevance of drawing a distinction between published and unpublished information, since such a distinction would overlook two important facts: “the fact that no one can know everything, and the fact that

104. Meg Leta Ambrose & Jef Ausloos, *The Right to Be Forgotten Across the Pond* 3 J. INFO. POL’Y 1, 14 (2012); see also Council Directive 95/46, *supra* note 90, at arts. 6(1)(e), 12(b), 14.

105. See *C.L. v. BCF Avocats d’affaires*, [2016] Q.C.C.A. 114 (Can.). The Quebec Commission d’Accès à l’Information (CAI), the government body responsible for the administration and enforcement of the Quebec DPL, recently provided some insight on its position with regards to the application of RTBF in Quebec and mentioned that it is doubtful that the RTBF, recognized in Europe, would find application in Quebec.

106. Teresa Scassa, *Journalistic Purposes and Private Sector Data Protection Legislation: Blogs, Tweets and Information Maps*, 35 QUEENS L.J. 733, 742 (2010). 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 also An Act Respecting the Protection of Personal Information in the Private Sector, R.S.Q. 1993, c P-39.1, s.1 (Can.); Personal Information Protection Act, S.A. 2003, c P-6.5, s. 1(1)(i) (Can.); Personal Information Protection Act, S.B.C. 2003, c 63, s.3(2) (Can.).

107. See, e.g., LINDOP, REPORT ON DATA PROTECTION IN THE U.K., 270, ¶¶ 31.02–.05. (1978) (examining public and private-sector computer systems, recommending a flexible legislative environment—with a set of broad principles guiding a data protection authority in its development of codes of practice aimed at various sectors of the economy).

108. *Id.*

people forget even what they once knew.”¹⁰⁹

In the U.K., a Data Protection Report from the late 1970s suggested that any piece of information about any data subject would at any given time be known only to a limited number of people.¹¹⁰ With Internet technologies, there is a spatial shift in the sense that physical spaces seem to dissolve and information can be available to a larger group of individuals. There is also a temporal shift in the sense that data can now be available for a longer period of time.

a. Spatial Shift

Since the conception of the Internet, the place where information is located has little impact on its accessibility. As soon as a document is available on a server, it can be found using general Internet search tools or other specialized tools. Trudel articulates the view that this changes the scale of threats to privacy on the Internet:

“Distance in space and the passage of time seem to have much less impact on the real availability of information. The Internet makes publication routine and information can easily be published outside of legitimate circles, thus the increased risk. Naturally, cyberspace is made up of both public and private spaces, but the reference points that distinguish between private and public have been blurred.”¹¹¹

Although personal records have been kept for centuries, only recently has the practice become a serious concern.¹¹² Until recently, public records were difficult to access since, for most of recorded history, they were only available locally.¹¹³ Following the Internet revolution, public records can be easily obtained and searched from anywhere.

109. *Id.*

110. *Id.* at ¶ 31.05 (“The truth is that any piece of information about any data subject will at any given time be known only to a finite number of people. The number may be large or small, but (with very few exceptions) it will never comprise the whole of the population of the United Kingdom. Moreover, as time passes the number will necessarily become smaller – by death and by forgetting – unless the information is circulated anew. In short, personal information is not just either ‘public’ or ‘private’: there is a wide range of possible knowledge among the public for any given item.”).

111. Pierre Trudel, *Privacy Protection on the Internet: Risk Management and Networked Normativity*, in REINVENTING Data Protection? 317, 326–27 (S. Gutwirth, et al. eds. 2009).

112. See Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1400–03 (2001) (a historical perspective on public sector databases and at 1403 to 1409 for a historical perspective on private sector databases).

113. Daniel J. Solove, *Access and Aggregation: Privacy, Public Records, and the Constitution*, 86 MINN. L. REV. 1137, 1142 (2002).

The United States federal courts, along with many state courts and agencies, are developing systems to place their records online.¹¹⁴ Solove suggests that while these records are readily available at local courthouses or government offices, placing them online has given rise to an extensive debate over privacy. In order to address these concerns, he suggests that we must rethink the accessibility of the information in public records.¹¹⁵ A recent complaint under PIPEDA involving Globe24h, a Romanian-based website,¹¹⁶ further illustrates the new risks pertaining to this increased accessibility. In that 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 (i.e. credit history, income, health information, etc.) included in these court decisions surfaced, in response to searches focusing on individuals' names.¹¹⁷ This case illustrates how access to court records is emblematic of the quantitative and qualitative changes generated by the Internet.

b. Temporal Shift

The Internet makes information available for longer periods of time—if not forever. Trudel articulates the view that with Internet technologies, there is a temporal shift.¹¹⁸ The persistence of information entails that pieces of data can outlive the context in which they were created and considered legitimate.¹¹⁹ For example, it may be legitimate for a piece of information to be available online to report a current news event, but archiving this information permanently on the Internet could trigger the situation where this information is then available for a period beyond what is necessary to report the event. He suggests that now that information can be found effortlessly, we have to reassess the arguments used to determine whether a given piece of information is public or private.¹²⁰ On this issue, Security Specialist Scheiner also suggests that part of the privacy concern nowadays relates to the fact that digital data can remain available indefinitely, since routine transactions such as credit card payments, paying tolls via

114. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PENN. L. REV. 477, 536 (2006); see also Solove, *supra* note 112, at 1409 (“Government agencies have begun to place records on their websites, and public records, once physically scattered across the country, can now be searched or gathered from anywhere in the country.”).

115. Solove, *supra* note 112, at 1456; see also Helen F. Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 131–32 (2004).

116. OFFICE OF THE PRIVACY COMMISSIONER OF CANADA, WEBSITE THAT GENERATES REVENUE BY REPUBLISHING CANADIAN COURT DECISIONS AND ALLOWING THEM TO BE INDEXED BY SEARCH ENGINES CONTRAVENED PIPEDA ¶ 1 (2015).

117. *Id.*

118. Trudel, *supra* note 40, at 328.

119. *Id.*

120. *Id.*

transponders, and opening OSN accounts such as Facebook, all generate digital records that are much easier and less expensive to store than to sort and delete.¹²¹ As a result, digital data never dies. That is very different than when fewer records or none at all were kept and after a while, people forgot details about particular incidents. He states: “We are a species that forgets stuff. . . . We don’t know what it is like to live in a world that never forgets.”¹²²

As the “lifespan” of personal information increases, so too does its dissemination. It is in response to these concerns that European countries have begun to entertain the adoption of laws that would allow individuals to request the deletion or removal of online data referring to or concerning them, also known as the RTBF.

II. CONSTITUTIONAL CHALLENGES WITH THE IMPLEMENTATION OF A RTBF

At first sight, the recognition in Canada of a RTBF does not sound that far-fetched. In fact, Canadian DPLs are modelled on European standards¹²³ 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 applying Directive 95/46/EC. 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 de-indexed from search engine results when certain conditions are met.¹²⁴

This situation raises 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 United States 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, Canadian courts would consider search engine results 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, it is reasonable to believe that the approach adopted in Europe would likely be considered

121. Tim Greene, *Schneier: Fight for Privacy or Kiss it Good-Bye*, CIO (Mar. 9, 2010, 7:00 AM), <http://www.cio.com/article/2419910/security0/schneier--fight-for-privacy-or-kiss-it-good-bye.html> [<https://perma.cc/LPP3-NRP6>].

122. *Id.*

123. GRATTON, *supra* note, at 14–21 (2013).

124. 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?*, 66 U. N.B. L. J. UNBLJ 185, 185–86, 196 (2015).

unconstitutional. While Canadian constitutional law allows for reasonable limitations of fundamental rights, this section explains how a European-style RTBF could hardly be justified under the criteria adopted by Canadian courts. It further explains how this RTBF may very well fail to strike an appropriate balance between freedom of expression and privacy and why private corporations may not be the adequate forums to address the fundamental issues at stake.

A. Freedom of Expression as a Constitutional Right

This section details the Canadian courts' role when Charter rights collide with each other or with non-Charter values, and the scope of freedom of expression in the context of personal information published online.

1. Court Intervention when Charter Rights Collide with Each Other: Oakes Test

Courts often intervene when Charter rights collide with each other or with non-Charter values.¹²⁵ 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.”¹²⁶ 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 to pursue collective goals of fundamental importance.¹²⁷

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.¹²⁸ This process applies to impugned statutes, regulations, and other enactments of general application.¹²⁹

The onus is always on the claimant to establish that the law encroaches upon one of his rights or the Charter rights. This generally involves interpreting the relevant provisions of the Charter to define the scope of the rights at stake and to determine

125. HOGG, *supra* note 48, at 36-12.

126. Canada Act, 1982, c 11 (U.K.), *reprinted in* R.S.C. 1985, app II, no 44 (Can.).

127. *R. v. Oakes*, [1986] 1 S.C.R. 103, 136 (Can.).

128. HOGG, *supra* note 48, at 38-2 to 3.

129. 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 S.C.R. 395, ¶¶ 36-55 (Can.); *see also* HOGG, *supra* note 48, at 38-13 to 14.

whether the activity of the claimant falls within the protected sphere of conduct.¹³⁰ 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.¹³¹ In this regard, the Supreme Court of Canada set out, in the seminal *Oakes*¹³² 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.¹³³ 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 the challenged provision’s meaning is ambiguous, courts may adopt a narrow interpretation so as to avoid a breach of the Charter.¹³⁴

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, 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.¹³⁵ For instance, this led the court to modify the tort of defamation, giving greater weight to the freedom of expression.¹³⁶ 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.

130. See HOGG, *supra* note 48, at 38-7; see also *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927, 967-968 (Can.).

131. Eloïse Gratton & Jules Polonetsky, *Privacy Above all Other Fundamental Rights?*, 6 (Apr. 28, 2016) (working paper), https://fpf.org/wp-content/uploads/2016/04/PolonetskyGratton_RTBFpaper_FINAL.pdf [<https://perma.cc/N6YT-H7GC>].

132. See *Oakes*, 1 S.C.R. at 138–40.

133. See HOGG, *supra* note 48, at 38-17 to -18.

134. *Id.* at 40-3 to -4; PIERRE-ANDRÉ CÔTÉ, *THE INTERPRETATION OF LEGISLATION IN CANADA* 498–99 (Carswell, 4th ed. 2011). For an example pertaining to freedom of expression, see *Canada (Attorney General) v. JTI-Macdonald Corp.*, [2007] 2 S.C.R. 610, ¶¶ 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, *supra* note 48, at 39-2 to 3, 39-9.

135. See *RWDSU v. Dolphin Delivery Ltd.*, [1986] 2 S.C.R. 573, 603 (Can.); *Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130, ¶¶ 91–98 (Can.).

136. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶¶ 38–65 (Can.).

2. The Scope of Freedom of Expression

Section 2(b) of the Canadian Charter provides that everyone has a fundamental right to the freedom of expression, including freedom of the press, and other media of communication.¹³⁷ The Charter is subject to a “purposive” and “generous” interpretation, which is meant to give full effect to the civil liberties that it guarantees.¹³⁸ Freedom of expression is no exception. The Court construed the notion of “expression” very broadly, so as to include any activity that attempts to convey meaning, including both form and content.¹³⁹

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.¹⁴⁰ Any rights or values that collide with freedom of expression must be analyzed 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 infringed, irrespective of the actual content that is targeted.¹⁴¹ This stems from the fact that 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.”¹⁴² In light of this principle, commercial advertisement is undeniably worthy of constitutional protection.¹⁴³ Even content such as false

137. Canada Act, 1982, c 11 (U.K.), *reprinted in* R.S.C. 1985, app II, no 44 (Can.).

138. *R. v. Big M Drug Mart Ltd.*, [1985] 1 S.C.R. 295, 344 (Can.).

139. *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927, 968–969 (Can.). 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 a by-law.

140. *R. v. Keegstra*, [1990] 3 S.C.R. 697, 733–734 (Can.).

141. *Irwin Toy Ltd.*, 1 S.C.R. 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).

142. *Keegstra*, 3 S.C.R. at 828.

143. *Ford v. Quebec (Attorney General)*, [1988] 2 S.C.R. 712, 766–767 (Can.) (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 S.C.R. 199 (Can.) (holding 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); *but see* *Canada (Attorney General) v. JTI-Macdonald Corp.*, [2007] 2 S.C.R. 610 (Can.) (upholding an anti-tobacco law which required tobacco manufacturers to place a warning attributed to the government on their products).

news,¹⁴⁴ hate speech,¹⁴⁵ and pornography¹⁴⁶ cannot be excluded from the reach of Section 2(b).¹⁴⁷ Violent acts, however, do fall outside the scope of freedom of expression.¹⁴⁸

The Supreme Court of Canada recognized the freedom of expression as essential to the functioning of our democracy, to seeking the truth in diverse fields of inquiry, and to our capacity for self-expression and individual realization.¹⁴⁹ As such, public interest has been construed broadly so as to include matters ranging from “politics to restaurant and book reviews.”¹⁵⁰

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.¹⁵¹ 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.¹⁵² 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.¹⁵³ As further discussed in this section, a RTBF may very well be

144. *R. v. Zundel*, [1992] 2 S.C.R. 731 (Can.).

145. *Saskatchewan (Human Rights Commission) v. Whatcott*, [2013] 1 S.C.R. 467 (Can.).

146. *R. v. Butler*, [1992] 1 S.C.R. 452 (Can.); *See also* *R. v. Sharpe*, [2001] 1 S.C.R. 45, ¶ 6 (holding that child pornography offences infringe freedom of expression but may be justified under s. 1 of the Charter. 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.).

147. HOGG, *supra* note 48, at 43-31 to 39.

148. *R. v. Keegstra*, [1990] 3 S.C.R. 697, 731 (Can.).

149. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶¶ 1, 47 (Can.); *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927, 968–969 (Can.); *Montréal (City) v. 2952-1366 Québec Inc.*, [2005] 3 S.C.R. 141, ¶ 74.

150. *Torstar*, 3 S.C.R. at ¶¶ 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 supra* Section A of this paper.

151. HOGG, *supra* note 48, at 43-13.

152. *Bou Malhab v. Diffusion Métromédia CMR Inc.*, [2011] S.C.R. 214, ¶¶ 20–21, 25 (Can.).

153. 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. *See* *Torstar Corp.*, 3 S.C.R. at 640, ¶¶ 65, 85, 96 (Can.); *see also* *WIC Radio Ltd. v. Simpson*, [2008] S.C.R. 420, 443, ¶ 28 (Can.). It should be noted that the civil law province of Quebec has different rules in regard to defamation. *See, e.g.*, *Néron v. Chambre des notaires du Québec*, [2004] 3 S.C.R. 95, 129, ¶ 56 (Can.). *See supra* Section I of this paper, which discusses this relevant legal framework.

considering infringing the constitutional right to freedom of expression of search providers, authors and webmasters, by hindering access to information.¹⁵⁴

Search engine operators. Search engines retrieve information from an immense pool of data and then organize and rank such information by displaying results. Therefore, little doubt exists 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.”¹⁵⁵ Such an activity undeniably conveys “meaning,” falling within the scope of Section 2(b).¹⁵⁶ Search engine results play an important role with respect to the exercise of freedom of expression in today’s world. The Supreme Court of Canada ruling about the essential role of hyperlinks provides useful insight:

[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.¹⁵⁷

In light of the above comments, there is little doubt that search

154. See Edward Lee, *The Right to Be Forgotten v. Free Speech*, I/S: J.L. & POL’Y INFO. SOC’Y, 7–8 CHI.-KENT L. REV. (forthcoming 2015) (with respect to the many persons—search providers, authors, webmasters, Internet users—whose freedom of expression might be infringed by the RTBF).

155. Lee, *supra* note 154, ¶ 30.

156. As a matter of comparison, a few United States 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, 586 (S.D.N.Y. 2013).

157. *Crookes v. Newton*, [2011] 3 S.C.R. 269 (Can.) (citing *SOCAN v. Canadian Assn. of Internet Providers*, [2004] 2 S.C.R. 427, 448 ¶ 40 (Can.) (citations omitted)). The Court refers to the publication rule of defamation law, which makes 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.

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 could be considered as violating 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.¹⁵⁸ 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 that repeatedly infringe copyrights.¹⁵⁹ Since the Charter does not apply directly to private corporations, it is reasonable to believe that authors could hardly challenge on constitutional grounds such decisions made by search engines.¹⁶⁰ 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.¹⁶¹

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. Likely, 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*,¹⁶² an unknown person attempted to dupe a national newspaper into publishing an allegedly forged bank document which, on its face, implicated the then Prime Minister of Canada in a serious financial conflict of

158. *RJR-MacDonald Inc. v. Canada (Att'y Gen.)*, [1995] 3 S.C.R. 199, ¶¶ 113, 124. Compare *Baidu.com*, 932 F.Supp.2d at 565–7, 586, where the United States 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 United States.

159. Lee, *supra* note 154, at 107.

160. 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.

161. See, e.g., Gianluigi Marino, *ITALY: Right to be Forgotten and the Google Advisory Council in Rome: Main Takeaways*, DLA PIPER (Sep. 11, 2014) <http://blogs.dlapiper.com/privacymatters/right-to-be-forgotten-and-the-google-advisory-council-in-rome-main-takeaways/> [https://perma.cc/SV5Z-SDPK] (about the legitimate expectation of authors that their works be disseminated via search engines).

162. *R. v. National Post*, [2010] 1 S.C.R. 477, ¶ 28 (Can.); See also *Edmonton J. v. Alberta (Att'y Gen.)*, [1989] 2 S.C.R. 1326, 1339–40 (Can.); see also *Ford v. Quebec (Att'y Gen.)*, [1988] 2 S.C.R. 712, 767.

interest. As the document involved constituted physical evidence reasonably linked to a serious crime, the police sought to subject this material to forensic analysis, and obtained a warrant in this regard. The Supreme Court of Canada confirmed the validity of the warrant, even if the result is to disclose the identity of the secret source. The Court 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.¹⁶³ However, in *Globe and Mail*,¹⁶⁴ the Court rejected the notion of a fundamental right to access to information. In this case, a national newspaper sought and obtained an exception—for one of its journalists—to the well-accepted rule of evidence that witnesses who are called to testify are obliged to answer the questions put to them, on the grounds that the journalist's testimony would reveal the identity of a confidential source. The Supreme Court held that the ban was not necessary to prevent a serious risk to the proper administration of justice. In light of this latter decision, it may 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, it could be reasonably argued that a RTBF would breach the constitutional right to freedom of expression of search engine operators, authors, and webmasters and that any law incorporating a European style RTBF would raise constitutional challenges, as discussed in Section B below.

B. Can the RTBF be a Justified Limit to Freedom of Expression?

As discussed in the previous Section 2, a RTBF would likely infringe the right to freedom of expression. This section 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

163. *National Post*, 1 S.C.R. ¶¶ 33, 40.

164. *Globe and Mail v. Canada (Att’y Gen.)*, [2010] 2 S.C.R. 592, ¶ 34 (Can.) (holding that Section 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).

enactment of general application. Accordingly, the analysis assumes 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 the legislator would implement it, and how far it would go in violating freedom of expression. For the purposes of this analysis, the RTBF will be analyzed as including the following features, as adopted in *Google Spain*:¹⁶⁵

- 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 pages published by third parties, and containing certain information relating to that person (i.e. delisting or deindexing);¹⁶⁶
- 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;¹⁶⁷
- The claimant does not have to show that the information causes prejudice;¹⁶⁸
- 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;¹⁶⁹
- 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;¹⁷⁰
- Search engine operators need to apply the above rules on a

165. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. ¶¶ 88–99; see also European Commission Press Release 14/EN WP 225, Guidelines on the Implementation of the European Union's Judgment on “*Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*” (C-131/12) (Nov. 26, 2014) (Spain) [hereinafter Press Release 14/EN WP 225].

166. See *Google Spain SL*, 2014 E.C.R. at ¶ 70.

167. *Id.* at ¶ 94.

168. *Id.* at ¶ 96.

169. *Id.* at ¶ 97.

170. *Id.*

case-by-case basis; and¹⁷¹

- 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.¹⁷²

The requirement from the Canadian Charter that the limitations be “prescribed by law” entails that the law provides sufficiently clear standards to avoid arbitrary applications.¹⁷³ 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 rarely strike down legislation on such a basis, even when limits are couched in vague terms,¹⁷⁴ and the analysis will therefore be conducted on the premise that the RTBF would pass this preliminary test.

At this point, each step of the *Oakes*¹⁷⁵ test will be examined to determine whether legislation providing for a RTBF may justify a limitation of the freedom of expression. Throughout the analysis, it should be considered that the Supreme Court of Canada has recognized that hyperlinks—and presumably, search results—have become essential tools to disseminate, find and access information.¹⁷⁶ 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-fulfillment.

The Supreme Court of Canada stressed in *Edmonton Journal* how important freedom of expression is to a democratic society and the right should only be restricted in very limited circumstances:

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

171. *Id.* at ¶ 99.

172. *Id.* at ¶ 77.

173. Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, *being* Schedule B to the Canada Act, 1982, c 11 (U.K.).

174. *See* HOGG, *supra* note 48, at 38–16 to 18. For a rare example of a law found to be void for vagueness, *see* *Crouch v. Snell*, [2015] N.S.S.C. 340, ¶ 130 (Can.), where the Nova Scotia Supreme Court struck down a provincial anti-cyberbullying act, which was held to provide no standard to avoid arbitrary decision-making. *See* discussion *supra* Section A.

175. *R. v. Oakes*, [1986] 1 S.C.R. 103, 135–40 (Can.).

176. *Crookes v. Newton*, [2011] 3 S.C.R. 269, ¶¶ 34–36 (Can.).

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.¹⁷⁷

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

1. Pressing and Substantial Objective

The first step of the *Oakes* test requires assessing whether the objective of the infringing measure is sufficiently important to justify overriding freedom of expression.¹⁷⁸ 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. The burden of proof is rather easy to satisfy in this regard.¹⁷⁹

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,¹⁸⁰ which are further discussed in Section 2. In *Google Spain*, the Court of Justice of the European Union 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.¹⁸¹ In other words, privacy is no longer protected by the mere difficulty of remembering or finding information,¹⁸² as would be the case with the hard copy of a newspaper published years ago.

The Supreme Court of Canada already acknowledged this problem. In *UFCW*,¹⁸³ a leading case on freedom of expression and privacy, the Court has highlighted that DPLs seek to avoid the "potential harm that flows from the permanent storage or unlimited dissemination of personal information through the Internet." The

177. *Edmonton J. v. Alberta (Att'y Gen.)*, [1989] 2 S.C.R. 1326, 1336 (Can.).

178. *Oakes*, 1 S.C.R. at 138.

179. See HOGG, *supra* note 48, at 38-22 to 23.

180. See Michael Douglas, *Questioning the Right to be Forgotten*, 40 ALTERNATIVE L.J. 109, 112 (2015).

181. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R. ¶ 80.

182. See Patricia Kosseim, Senior Gen. Counsel & Dir. Gen., Legal Servs., Policy, Research & Techn. Analysis Branch, Office of the Privacy Comm'r of Canada, Address at the Yukon Bench and Bar Seminar: The (In)finite Life of Personal Information in a Digital Age (Sept. 10, 2015).

183. *Alberta (Info. and Privacy Comm'r) v. United Food and Com. Workers, Loc. 401 (UFCW)*, [2013] 3 S.C.R. 733, ¶ 23 (Can.).

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.¹⁸⁴ Such an objective is connected to fundamental values, such as privacy, dignity and autonomy.¹⁸⁵ In all likelihood, this objective would be recognized as sufficiently important to justify a limit on freedom of expression.

2. Rational Connection Between the Law and Its Objective

This second requirement from *Oakes* aims 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 sufficiently make this demonstration. At this stage, there is no need to prove the efficiency of the impugned law.¹⁸⁶ Again, the low threshold presents very few cases where a law has been nullified under it.¹⁸⁷

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, most likely not be the subject of extensive debate.

3. Minimum Impairment

The third step of the *Oakes* test is usually the most difficult to satisfy. It requires a showing that the law impairs the right in question “no more than necessary to accomplish the desired objective.”¹⁸⁸ In other words, the question is whether the same goal could possibly be achieved in a significantly less infringing manner.¹⁸⁹ The legislator is, however, given some leeway. To the

184. See GRATTON, *supra* note 85, at 201–02 (on the notion that data protection laws should aim at protecting information that can create a risk of harm to individuals¹²³); see also ONLINE REPUTATION, *supra* note 84, at 5 (with regard to the purpose of the RTBF).

185. *UFCW*, 3 S.C.R. ¶ 19.

186. *Alberta v. Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. 568, ¶ 48 (Can.).

187. HOGG, *supra* note 48, at 38–34.1; see also *Saskatchewan (Human Rights Commission) v. Whatcott*, [2013] 1 S.C.R. ¶ 92 (Can.) (This is a noteworthy exception where the Supreme Court of Canada declared a limitation to freedom of expression invalid for lack of rational connection. 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.).

188. HOGG, *supra* note 48, at 38–36.

189. *Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. at ¶¶ 66 (Can.); see also *Carter v. Canada (Att’y Gen.)*, [2015] 1 S.C.R. 331, ¶ 102 (Can.).

extent that the law falls within a range of reasonable, less drastic alternatives, it will pass the test, even though the objective could be accomplished in a slightly less infringing manner.¹⁹⁰ Despite the leeway given to the legislator, however, the RTBF 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”¹⁹¹—are probably too broad and subjective, and would necessarily result in delisting information of public interest beyond the objective sought by the legislator:

- **Inadequate.** What is “adequate” for one might not be for another. Apart from content such as child pornography, “revenge porn,” and Magnotta-like videos,¹⁹² little consensus exists as to the definition of “inadequate” information on the Internet. One might also wonder to what extent alleged inaccuracies make the information “inadequate.”¹⁹³ The accuracy of the information might be difficult to verify, as is often the case in matters of defamation. For instance, it is not clear if the search provider would be expected to conduct some kind of investigation, or if instead the claimant’s allegations should be taken at face value. Pursuant to such criteria, it seems that a mere appearance of “inadequacy” might be enough to hinder access to content of an inherently public interest character.
- **Irrelevant.** Nothing is more subjective than relevance. For example, it is not clear to whom is the information supposed to be relevant for, and in what respect. What is “relevant” for one might not be for another. It may vary greatly depending on the context or across jurisdictions. Some have raised the concern that 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 and free

190. *Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. ¶¶ 53–55.

191. For our purposes, we will not consider 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 Press Release 14/EN WP 225, *supra* note 165.

192. Canadian Press, *Luka Magnotta Video: Gore-Site Owner Conditionally Sentenced*, HUFF. POST (Jan. 25, 2016, 10:42 AM), http://www.huffingtonpost.ca/2016/01/25/trial-begins-in-edmonton-for-gore-site-owner-who-posted-magnotta-video_n_9066948.html [https://perma.cc/TH2K-H5VX].

193. In matters of personal information, accuracy and adequacy are considered to be closely related. See Press Release 14/EN WP 225, *supra* note 165, at 15.

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"?¹⁹⁴

- **No longer Relevant.** It is not clear when information would lose relevance—and whether this would be after five years, ten years, fifteen years, or any longer period. If some case, the deindexed information may later regain 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.¹⁹⁵ As for crimes, it is also unclear if some distinctions should be made between different types of crimes.
- **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. It may be difficult to conclude that the processing is "excessive" in regard to its purpose, when the main purpose 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, although the scope of "public life" is unclear. For instance, it may be limited to politicians and elected officials, or it may in some cases extend to public servants, business people, professionals, journalists, as well as well-known artists and athletes. It is also debatable whether local, national, and international public figures should be treated on an equal basis, whether the search provider would be expected to conduct research to determine whether the claimant plays a role in public life, or how the criteria should be otherwise assessed.

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

According to the Article 29 Working Party's guidelines released in November 2014, for implementing the *Google Spain* decision, interpretations should be made within existing national

194. Peston, *supra* note 11, at 4.

195. See Patricia Sánchez Abril & Jacqueline D. Lipton, *The Right to Be Forgotten: Who Decides What the World Forgets?*, 103 KY. L.J. 363, 383 (2014–15).

law.¹⁹⁶ Interpretation resulted in inconsistent outcomes across the EU. Leta Jones explains: “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.’”¹⁹⁷ The guidelines provide a set of criteria for data-protection authorities handling RTBF complaints to follow, but some of the questions might have a different answer in the different countries, given the vagueness of the criteria behind the RTBF.

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 Code¹⁹⁸ 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 expression more than necessary to secure the legislation’s objectives.¹⁹⁹ Recently, the Nova Scotia Supreme Court held that an anti-cyber bullying act failed to define cyber bullying so as to avoid over breadth.²⁰⁰

In the matter at hand, the vague criteria is compounded by the reality that the private corporations would enforce the RTBF. As many commentators have pointed out, these corporations have an incentive to err on the side of removal to reduce costs and/or to avoid legal liability and the hefty fines to which they are exposed in case of non-compliance.²⁰¹ This should give us pause as to the reasonableness of entrusting private entities with the tasks of arbitrating fundamental rights and determining what is in the public interest, with little or no government or judicial oversight.²⁰² Without transparency and openness, nothing guarantees the integrity of the process.²⁰³

In addition, the process adopted in *Google Spain* appears to be biased in favor of the claimant, thus increasing the likelihood that

196. 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 2015 O.J. (179/16/EN).

197. Jones, *supra* note 24, at 173.

198. Criminal Code, R.S.C. 1985, c. C-46 (Can.).

199. R. v. Zundel, [1992] 2 S.C.R. 731, 768–775 (Can.).

200. Crouch v. Snell, [2015] N.S.S.C. 340, ¶ 165 (Can.).

201. European authorities may impose fines for non-compliance with privacy legislation. See, e.g., Cunningham, *supra* note 11, at 24; Douglas, *supra* note 180, at 110; Abril & Lipton, *supra* note 195, at 382–385; *supra* Section 2.

202. Abril & Lipton, *supra* note 195, at 366.

203. Note, the Supreme Court of Canada recognized the importance of openness for the proper administration of justice. See, e.g., Canadian Broadcasting Corp. v. Canada (Att’y Gen.), [2011] 1 S.C.R. 19, ¶ 29 (Can.). Similarly, in light of the fundamental values at stake, some level of transparency could be considered as necessary in implementing the RTBF.

information of public interest will be 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.²⁰⁴ Moreover, while claimants can resort to privacy authorities and to the courts if dissatisfied with the decision, nobody else can challenge it.²⁰⁵ This one-sided approach breaches 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.²⁰⁶

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. Perhaps, the presumption should instead play in favor of freedom of expression, as this approach would be more consistent with Canadian case law.

For instance, in *Edmonton Journal*,²⁰⁷ the Supreme Court of Canada struck down provisions of a law that 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*,²⁰⁸ while balancing the values underlying the freedom of expression against the right to reputation, the Court gave priority to the former in broadening the defenses against

204. Google has nevertheless decided to notify webmasters that a link has been removed. See Cunningham, *supra* note 11, at 27; see also Press Release 14/EN WP 225, *supra* note 165, at 10.

205. See Leonid Sirota, *The Power of Google, Squared*, DOUBLE ASPECT (Mar. 16, 2015), <https://doubleaspect.blog/2015/03/16/the-power-of-google-squared/> [<https://perma.cc/PH8U-DCDL>] (citing Andrew McLaughlin, former CEO of Digg and former Director of Public Policy for Google); see also Release 14/EN WP 225, *supra* note 165, at 7.

206. 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 v. Can. (Att'y Gen.)*, [2010] 2 S.C.R. 592, ¶¶ 74–75 (Can.). We believe that the same logic should apply, to some extent, to the removal of links pointing toward authors' works.

207. *Edmonton J. v. Alta. (Att'y Gen.)*, [1989] 2 S.C.R. 1326, 1346–1350 (Can.).

208. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶ 65 (Can.) (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).

defamation.

Finally, the fact that an individual using his or her RTBF has no obligation to demonstrate any prejudice or even a mere risk of harm should be considered.²⁰⁹ The claimant should have the burden of showing that the dissemination of his or 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.

As proposed, the RTBF is not 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, unnecessarily restricting 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 de-indexed 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 there are 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.

4. Proportional Effect

The fourth and final step of the *Oakes* analysis is to determine whether the deleterious effects of the infringement are proportionate to their benefits.²¹⁰ Given the conclusion that the RTBF is not minimally impairing, it would not be necessary to examine this requirement. However, for the purposes of this analysis, we will proceed with this last part of the analysis, assuming a RTBF would satisfy the first three criteria.

Proportional effect is rarely an issue when the first three criteria are met.²¹¹ Nevertheless, a RTBF would most likely fail under this last step, especially considering comments made by the Supreme Court of Canada in *UFCW*,²¹² one of the few cases where a law was struck down on that ground. In *UFCW*, the question was

209. In Europe, the non-binding Article 29 Data Protection Working Party Guidelines do suggest considering "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 Press Release 14/EN WP 225, *supra* note 165, at 18.

210. *Alberta v. Hutterian Brethren of Wilson Colony*, [2009] 2 S.C.R. 567, ¶¶ 72–76 (Can.).

211. HOGG, *supra* note 48, at 38-43 to 44.

212. *Alberta (Info. & Privacy Comm'r) v. United Food and Com. Workers, Loc. 401 (UFCW)*, [2013] 3 S.C.R. 733 (Can.).

whether the Alberta DPL, the *Personal Information Protection Act*, could prevent a union from videotaping and photographing individuals crossing the picket line during a strike. As is the case with the RTBF, the Alberta DPL protects *all* information about an identifiable individual. The Supreme Court of Canada gave little weight to the benefits of the law in terms of privacy.²¹³ The Court observed that the statute's definition of "personal information" was over-inclusive as it includes any information related to an individual, regardless of its context, even if no intimate details are revealed.²¹⁴ Under these circumstances, the Court gave priority to the union's freedom of expression and declared the statute invalid.²¹⁵

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.²¹⁶ It is restricted to a "biographical core of information," which includes "intimate personal details."²¹⁷ Moreover, an individual is only entitled to a "reasonable expectation of privacy," which may vary depending on the context.²¹⁸ Even under the Quebec *Charter of Human Rights and Freedom* (the "Quebec Charter"), which expressly guarantees the right to privacy, the purpose of the protection is to allow for a "sphere of personal autonomy" in regards to "choices that are of a fundamentally private or inherently personal nature."²¹⁹ It does not protect every piece of data related to an identifiable individual.

In other words, a RTBF may be considered as covering 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

213. *See id.*

214. *Id.* at ¶¶ 25–26.

215. *Id.* at ¶¶ 37–41. Alberta's *Personal Information Protection Act* 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." *See Cunningham, supra* note 11, at 29–31; GRATTON, *supra* note 85, at 93–106 (with respect to the over-inclusiveness of the definition of "personal information").

216. *See Power, supra* note 82, at 237–240.

217. *R. v. Plant*, [1993] 3 S.C.R. 281, 293 (Can.).

218. *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, 159 (Can.).

219. *Aubry v. Vice-Versa*, [1998] 1 S.C.R. 591, ¶¶ 52–57 (Can.) (holding that the public's right to information, supported by freedom of expression, places limits on the Quebec Charter's right to privacy). For further discussion of the Quebec privacy legal framework and this case *see supra* Section A.

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.²²⁰ As such, it could be reasonably argued that 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.²²¹ As the Court put it, with respect to the right to reputation,²²² “freewheeling debate on matters of public interest is to be encouraged, and must not be thwarted by ‘overly solicitous regard for personal reputation.’”²²³

One may reasonably argue that 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. Therefore, a RTBF may well 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),²²⁴ its benefits might justify such purposive limits on the freedom of expression.

In light of the foregoing, because a RTBF, at least as defined in Europe, is very broad without justifications, Canadian courts may very likely find that such RTBF infringes upon the right to freedom of expression in a way that cannot be justified under Section 1 of the Canadian Charter.²²⁵ Accordingly, any law

220. Leonid Sirota, *The Power of Google*, DOUBLE ASPECT (Sept. 21, 2014), <https://doubleaspectblog.wordpress.com/2014/09/21/the-power-of-google/> [<https://perma.cc/8QHB-WUGM>].

221. *Sask. (Hum. Rights Comm’n) v. Whatcott*, [2013] 1 S.C.R. 467, ¶ 109 (Can.) (where the Supreme Court of Canada declared parts of Alberta’s anti-hate speech provisions invalid).

222. The Supreme Court of Canada has stated that the right to reputation is “intimately” related to privacy. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶ 59 (Can.).

223. *Id.* at ¶ 52.

224. In fact, Google has already taken steps to cope with the “revenge porn” phenomenon. *See Lee, supra* note 154, at 19–22 (The author also suggests that protecting victims of traumatic crimes might be a justifiable purpose for a limited right to be forgotten.).

225. *See Charter, supra* note 50. However, 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

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 de-indexed from search results. When possible, courts will avoid an interpretation that would be inconsistent with the Constitution of Canada.

III. IMPLEMENTATION OF A RTBF IN QUEBEC

Quebec, a primarily French-speaking province, has the most privacy-friendly and stringent reputation legal framework in place in Canada, and the most highly developed case law in this field. Quebec was the first province to enact a DPL for the private sector in 1993²²⁶ and has additional statutes that regulate the publishing of personal information. For instance, the Quebec²²⁷ Charter and the *Civil Code of Quebec* (“C.C.Q.”)²²⁸ are being relied upon by plaintiffs to address invasion of privacy and revenge porn activities.²²⁹ Some could therefore expect a RTBF to be more easily implemented in this province, although there are two main challenges with such implementation. The test used in *Google Spain* to determine if information should be de-indexed is different than the test provided for under Quebec law when determining if personal information may be published in the first place. Moreover, while under the RTBF a private sector search engine may be in charge of making the assessment, under Quebec law the courts are in charge of making this assessment. While Quebec protects online privacy and reputation better than the rest of Canada, there are also limits to the efficiency of the Quebec legal framework in addressing concerns at the heart of a RTBF.

A. *Challenges with the Implementation of a RTBF Under Quebec Law*

In Quebec, the right to privacy has been elevated to the rank of a fundamental right protected by the Constitution.²³⁰ The Quebec Charter uniquely guarantees everyone the “right to respect for his

of the public to assert their rights.

226. Act Respecting the Protection of Personal Information in the Private Sector, C.Q.L.R., c P-39.1 (Can. Que.).

227. Quebec Charter of Human Rights and Freedoms, C.Q.L.R., c C-12 (Can.) [hereinafter Quebec Charter].

228. *Id.*

229. Section A elaborates on some of these privacy cases. As for “revenge porn” cases, see, e.g., J.G. c. M.B., [2009] Q.C.C.S. 2765 (Can.); L.D. c. J.V., [2015] Q.C.C.S. 1224 (Can.).

230. ÉDITH DELEURY & DOMINIQUE GOUBAU, LE DROIT DES PERSONNES PHYSIQUES 173 (Yvon Blais, 5th ed. 2014) (quoting ÉDITH DELEURY & DOMINIQUE GOUBAU, LE DROIT AU RESPECT DE LA VIE PRIVÉE (Yvon Blais, 3rd ed. 2003).

private life,”²³¹ and any unlawful infringement may entitle the victim to an injunction or to damages.²³² This Quebec Charter is deemed “quasi-constitutional” because it has priority over inconsistent provincial laws, making the latter inoperative.²³³ However, unlike the Canadian Charter, ordinary legislative amendments can change the Quebec Charter.

Articles 3, 35, and 36 of the C.C.Q. also protect the right to privacy. Article 35 C.C.Q., states that “[e]very person has a right to the respect of his reputation and privacy.” This illustrates the principle outlined in Article 5 of the Quebec Charter.²³⁴ Article 36 C.C.Q. 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.”²³⁵

1. “Public Interest” Test

The *Google Spain* case established a precedent under which European residents have a right to stop search engines from providing links to information about them deemed irrelevant, no longer relevant, inadequate, or excessive. Quebec law already introduced a framework that provides a test to be used to determine if personal information may be published and therefore, posted online. This test from the C.C.Q. pertains to whether the information is “legitimate information of the public.” It is therefore different than the “inadequate, irrelevant, or no longer relevant” test proposed in the *Google Spain* case, which is meant to determine if the content should be de-indexed when a certain name is searched.

Quebec courts have characterized the right to privacy as “one of the most fundamental rights related to personality.”²³⁶ That said,

231. See Quebec Charter, *supra* note 227, s. 4–5; see also *Aubry v. Éditions Vice-Versa Inc.*, [1998] 1 S.C.R. 591 (Can.) (with respect to the scope of the right to privacy under the Quebec Charter, 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 case, the Court reached the conclusion that the girl’s right to privacy outweighed the artist’s freedom of expression).

232. See Quebec Charter, *supra* note 227. Since the Quebec Charter applies to private persons, an individual could technically, 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. 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.

233. See Alberta Bill of Rights, R.S.A. 2000, c A-14, s. 2; see also Quebec Charter, *supra* note 227, s. 52 (in balancing conflicting rights, Quebec courts apply Section 9.1 of the Quebec Charter, which is the equivalent of § 1 of the Canadian Charter).

234. *DELEURY & GOUBAU*, *supra* note 230, at 177.

235. Several cases have considered this limitation and they are discussed in *supra* Section A.

236. See, e.g., *The Gazette (division Southam) v. Valiquette*, 1996 CanLII 6064 (Can. Que.).

as with any other right, the right to privacy is not absolute and must be balanced with other fundamental rights, including freedom of expression. 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.²³⁷ Quebec’s evolving case law has been providing guidance on how to balance these rights.

In a landmark case *Aubry v. Éditions Vice-Versa Inc.*,²³⁸ the Supreme Court of Canada ruled 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.”²³⁹ The Court explained:

This 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.²⁴⁰

The Court articulated 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.”²⁴¹ 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.²⁴² 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.”²⁴³ This view confirms that the approach to invasion of privacy focuses on the concept of *public interest*, which is a complex

237. *A. v. Corporation Sun Media*, [2009] Q.C.C.Q. 3263 (Can.).

238. *Aubry v. Éditions Vice-Versa Inc.*, [1998] 1 S.C.R. 591 (Can.).

239. *Id.* at ¶ 57.

240. *Id.*

241. *Id.* at ¶ 58.

242. *Id.*

243. *Id.*

and evolving concept, as explained by Professor Trudel:

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.²⁴⁴

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 content in which the public has a legitimate interest.”²⁴⁵ In *Société Radio-Canada v. Radio Sept-Îles, Inc.*,²⁴⁶ Justice LeBel (then at the Quebec 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.²⁴⁷

Courts will sometimes take the position that the right to privacy has been infringed, even if the information published is of public interest, notably in situations where the information has been obtained by breaching the individual’s privacy rights,²⁴⁸ illustrating that privacy is considered as an important right.

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.²⁴⁹ In recent decisions,

244. Pierre Trudel, *L’oubli en Tant que Droit et Obligation dans les Systèmes Juridiques Civilistes* (2013) (unpublished text prepared for Université de Montréal), <http://pierretrudel.openum.ca/files/sites/6/2016/08/NotesoubliREV-1.pdf> (free translation) [<https://perma.cc/J6FH-NR4R>].

245. *Id.*

246. *Société Radio-Canada v. Radio Sept-Îles, Inc.*, [1994] Q.C.C.A. 5883 (Can. Que.).

247. *Id.*

248. *A v. Corporation Sun Media*, [2009] Q.C.C.Q. 3263 (Can.).

249. *See Gazette v. Goulet*, [2012] Q.C.C.A. 1085 (Can.) (the appellants used a file

some courts interpreted the notion of “legitimate information of the public” very narrowly when assessing the legality of published pictures,²⁵⁰ which illustrates the challenge inherent in always striking the right balance. 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.²⁵¹ This sets a favorable precedent for freedom of expression.

In online publications, an important concern is the protection of reputation. The Supreme Court of Canada recognized that the protection of reputation is “intimately related” to the protection of personal privacy.²⁵² 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.²⁵³ Recovery for defamation, however, is barred if the statements are true,²⁵⁴ even if they are embarrassing, and

photo identifying the respondent in uniform standing in the doorway of the penitentiary he guards, 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, e.g.*, *Bloc v. Sourour*, [2009] Q.C.C.A. 942 (Can.).

250. *See Hammedi v. Cristea*, [2014] Q.C.C.S. 4564 (Can.). Many authors have 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. *See Pierre Trudel, Portée Excessive du Droit à L'image*, J. MONTRÉAL (Sep. 25, 2014, 8:14 AM), <http://www.journaldemontreal.com/2014/09/25/portee-excessive-du-droit-a-limage> [<https://perma.cc/4MUQ-8R2M>]; *see also* Eloïse Gratton, *A Picture is Worth a Thousand Words*, ELOÏSE GRATTON (Sep. 26, 2014, 2:27 PM), <http://www.eloïsegratton.com/blog/2014/09/26/a-picture-is-worth-a-thousand-words/> [<https://perma.cc/UT3D-S7JT>]; Leonid Sirota, *Une Image et Mille Maux*, DOUBLE ASPECT (Oct. 10, 2014), <https://doubleaspectblog.wordpress.com/2014/10/10/une-image-et-mille-maux/> [<https://perma.cc/9G6S-ELSZ>].

251. *See Blanc v. Editions Bang Bang*, [2011] Q.C.C.S. 2624 (Can.) (holding 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] Q.C.C.Q. 5799 (Can.) (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).

252. *See Hill v. Church of Scientology of Toronto*, [1995] 2 S.C.R. 1130, ¶ 121 (Can.).

253. *See, e.g.*, *Slanderous Reports Act 1275*, 3 Edw. 1 c. 34 (Eng.); *see also* *A Brief Narrative of the Case and Tryal of John Peter Zenger*, Printer N.Y. Wkly. J. (1734) (establishing the precedent of truth as an absolute defense to defamation), <http://oll.libertyfund.org/pages/1736-brief-narrative-of-the-trial-of-peter-zenger> [<https://perma.cc/7F3V-92AU>].

254. Robert Kirk Walker, *The Right to be Forgotten*, 64 HASTINGS L.J. 257, 262 (2012) (discussing *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)).

regardless of the level of malice intended by the speaker.²⁵⁵

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 from the public gaze.”²⁵⁶ 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.²⁵⁷ This being said, in Quebec, the accuracy of the information revealed to the public (or the fact that it is true) does not suffice to avoid civil liability.²⁵⁸ In that sense, the Quebec legal framework better protect individuals’ reputations, 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 additional layer of protection helps to further enhance the protection of individual reputations.

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.²⁵⁹ The more an online publication relates to significant political issues, the more broadly the rights to freedom of opinion and expression are interpreted.²⁶⁰ Consequently, even without a 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*, where it cited an excerpt from author 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.”²⁶¹

The definition of the “public interest” in common law

255. *Id.*

256. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶ 59 (Can.) (emphasis in original). Certain common law provinces have enacted specific laws dealing with defamation. *See* Ontario Libel and Slander Act, R.S.O. 1990, c L.12 (Can.); British Columbia Libel and Slander Act, R.S.B.C. 1996, c 263 (Can.); Libel and Slander Act, R.S.O. 1990, c L.12 (Can.).

257. ONLINE REPUTATION, *supra* note 84, at 9–10.

258. *See, e.g.*, *Société TVA, Inc. v. Marcotte*, [2015] Q.C.C.A. 1118, ¶ 99 (Can.).

259. *Bou Malhab v. Diffusion Métromédia CMR, Inc.*, [2011] 1 S.C.R. 214 (Can.); *see also* *Rosenberg v. Lacerte*, [2013] Q.C.C.S. 6286 (Can.).

260. *Lafferty, Harwood & Partners c. Parizeau et al.*, [2003] Q.C.C.A. 32941, ¶ 155 (Can.); *Rosenberg v. Lacerte*, [2013] Q.C.C.S. 6286, ¶ 141 (Can.).

261. *Crookes v. Newton*, [2011] 3 S.C.R. 269, ¶ 37.

jurisdictions is generally in line with the one prevailing in Quebec. In *Grant v. Torstar Corp.*,²⁶² 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.”²⁶³ 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.”²⁶⁴

In short, by emphasizing public interest, Canadian courts have generally been able to strike an appropriate balance between the two competing rights at the heart of a RTBF—the right to privacy and freedom of expression—when assessing the legitimacy of a publication involving personal information. In case of conflict between these two fundamental rights, the notion of *public interest* is used to allow courts to determine whether the public has a genuine stake in knowing about the private information that is being revealed to the public.²⁶⁵

2. Courts Outsourcing the Balancing of Rights

Under the proposed RTBF in *Google Spain*, search engines are the parties in charge of interpreting the new standard and must unilaterally determine the balance between the value of information being published and the impact on a user. Google’s role as the *de facto* decision-maker of these value-laden societal issues is raising much concern,²⁶⁶ especially since Google has admitted to be struggling with implementing the ruling,²⁶⁷ and has also publicly confessed missteps in its attempted compliance.²⁶⁸

262. *Grant v. Torstar Corp.*, [2009] 3 S.C.R. 640, ¶¶ 38–65 (Can.).

263. *Id.* at ¶ 105.

264. *Id.*

265. *Id.* at ¶ 102.

266. Catherine Baksi, *Right To Be Forgotten “Must Go,” Lords Committee Says*, L. GAZETTE (July 30, 2014), <http://www.lawgazette.co.uk/law/right-to-be-forgotten-mustgolordscommittee-says/5042439> [<https://perma.cc/2F8V-W32Q>] (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).

267. Loek Essers, *This is How Google Handles ‘Right to be Forgotten’ Requests*, COMPUTERWORLD (Nov. 19, 2014, 12:54 PM), <http://www.computerworld.com/article/2849686/this-is-how-google-handles-right-to-be-forgotten-requests.html> [<https://perma.cc/B4YQ-FYVJ>]; GOOGLE ADVISORY COUNCIL, ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN (2015) (right after the RTBF decision, Google convened an advisory council); *see also* ONLINE REPUTATION, *supra* note 84, at 5.

268. *See* Caroline Preece, Rosie Clarke, & Joe Curtis, *Google ‘Right to be Forgotten’: Everything You Need to Know*, ITPRO (Feb. 9, 2015), <http://www.itpro.co.uk/security/22378/google-right-to-be-forgotten-everything-you-need-to-know> [<https://perma.cc/Y4FV-JMXE>] (quoting Google’s chief legal officer as saying

Under the existing framework in Quebec, courts properly balance the right to privacy and reputation against the right to freedom of information and freedom of expression. As discussed above, this has often proven to be a challenging and difficult task, one that has a huge impact on the fundamental rights (privacy and freedom of expression) of individuals, as well as on the value of freedom of information. This complexity makes for an even stronger argument against allowing or empowering a third, private sector entity, to decide on these complex issues.

In her new book, *Ctrl+Z: The Right to Be Forgotten*, Professor Leta Jones explains “when information is made public, a court or agency order should be required for right-to-be-forgotten removal requests.”²⁶⁹ In her opinion, intermediaries are not the optimal party to be assessing oblivion claims:

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.²⁷⁰

Courts and government authorities are usually the ones that should 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.²⁷¹ In 2011, the Supreme Court of Canada rendered an important decision regarding hyperlinking.²⁷² 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

“[o]nly 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”). See also Cunningham, *supra* note 11, at 28–29.

269. JONES, *supra* note 24, at 179.

270. *Id.*

271. For example, the Federal Court of Canada recently issued a decision in *A.T. v. Globe24h.com*, [2017] F.C. 114 (Can.), illustrating that courts should be the ones issuing orders to remove information from Google search results.

272. *Crookes v. Newton*, [2011] 3 S.C.R. 269 (Can.).

would have the effect of seriously restricting the flow of information and, as a result, freedom of expression.”²⁷³ However, the Court noted 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.²⁷⁴ It is not clear if such a balanced approach would have been considered in a context where the decision of 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.

Adding to allegations of censorship, data controllers have no obligation under either the *Google Spain* case or the Directive 95/46/EC to alert webmasters that links to their pages have been delisted,²⁷⁵ and allegedly EU officials were even discouraging Google from giving such notices.²⁷⁶ In most cases, the most informed advocate for why information should be available is the publisher of the content.²⁷⁷ 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 judgments 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, through the RTBF, would thus be 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. As suggested by Professor Floridi, the RTBF is a half-baked solution, and “[i]f Europe really wanted to regain control over personal data, giving Google this type of power is an odd outcome.”²⁷⁸

It is not to say that search engines have no role to play on the issue of protecting privacy and reputation online. They may have a

273. *Id.*

274. *Id.* at ¶ 40.

275. Case C-131/12, *Google Spain SL v. Agencia Española de Protección de Datos*, 2014 E.C.R.; *but see GDPR, supra* note 3, art. 17 (requiring data controllers to notify third parties of requested deletions).

276. *See* Toobin, *supra* note 11 (citing objections from the Article 29 Working Party to “Google’s practice of informing publishers when links that individuals objected to were deleted”); *see also* Cunningham, *supra* note 11, at 27.

277. Although organizations hosting or publishing content online may not have the incentive to expend the resources necessary to demonstrate that the information is still relevant. Note, the result of the proposed GDPR 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. Under the RTBF, the claimant seeking data erasure has no obligation to prove the information’s irrelevancy.

278. *See* Mark Scott, *Europe Tried to Rein in Google. It Backfired.*, N.Y. TIMES (Apr. 18, 2016), <https://nyti.ms/2ohPzsl> [<https://perma.cc/P939-QDF7>].

role to manage content that is illegal. For example, Google has decided to provide a web form on Google.com to enable victims of revenge porn to have it removed from search results based on their names.²⁷⁹ Mug shot extortion sites appeared, attempting to extort money from individuals with an arrest record by publishing their photos and names, and demanding money to remove the record,²⁸⁰ and Google has altered its search algorithms to reduce such sites' salience.²⁸¹ Such initiatives have not raised any controversy.

B. *Limits to the Efficiency of Quebec Law*

While the Quebec legal framework provides for a more stringent framework on the issue of online privacy and reputation, it also has some limits. There are significant limitations to judicial recourse²⁸² and, as raised by the OPC: "once information has been posted online, there is never any guarantee that it has not been reposted elsewhere on the Internet."²⁸³

As discussed previously in Section A, the default rule in Quebec is that the information cannot be published without the individuals' prior consent or unless the information is of "legitimate interest of the public," which is a relatively stringent test compared to common law jurisdictions. Still, it should be noted that the "public interest" test will be used at the point which the information is either published, or upon a plaintiff seeking the removal of the content before a court of justice. The public interest of the information published is therefore evaluated at a specific period of time. A court that takes the view that certain information is of public interest on a specific date, may have reached a different conclusion ten years later when the information may be outdated,

279. Amit Singhal, 'Revenge Porn' and Search, GOOGLE PUB. POL'Y BLOG (June 19, 2015), <http://googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html> [<https://perma.cc/R3ZZ-LAB9>].

280. Jane E. Bobet, *Mug Shots and the FOIA: Weighing the Public's Interest in Disclosure Against the Individual's Right to Privacy*, 99 CORNELL L. REV. 633, 634–35 (2004).

281. Barry Schwartz, *Google Launches Fix to Stop Mugshot Sites from Ranking: Google's MugShot Algorithm*, SEARCH ENGINE LAND (Oct. 7, 2013, 9:36 AM), <http://selnd.com/2nRtZhl> [<https://perma.cc/BK79-649K>].

282. ONLINE REPUTATION, *supra* note 84, at 9–10 (for instance, the OPC has raised the point that the cost of pursuing litigation may not make this type of remedy accessible for everyone).

283. *Id.* at 6. In *Laforest v. Collins*, [2012] Q.C.C.S. 3078 (Can.), the Superior Court of Quebec addressed the concern that negative comments could be reposted elsewhere on the Internet by ordering 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. This type of order may become increasingly useful in future online defamation cases.

and there is no process to “reopen” the assessment of the information at a later time.

Such a process may be considered, but it would raise two main challenges, namely the issues of *res judicata* and limitation periods, which issues would also need to be addressed. There is also no process to restore data if the information, after being removed, becomes of public interest over time, or at a later date.

1. *Res Judicata* and Prescription/Periods of Limitations

First, in the event that an individual has unsuccessfully instituted legal proceedings to prevent the publication of an article on the grounds that the content is not of public interest, this individual would be “estopped,” by virtue of the doctrine of *res judicata*, from instituting new proceedings at a later point in time unless the information is republished. The doctrine of *res judicata* is a fundamental doctrine of the justice system in Canada that can be divided in two distinct forms: issue estoppel and cause of action estoppel.²⁸⁴ Under the former, a litigant is estopped when the issue has clearly been decided in a previous proceeding. Under the latter, a litigant is estopped when the cause of action has passed into a matter adjudged in a previous proceeding.²⁸⁵ These two distinct forms of *res judicata* could have a significant impact in a situation where, for instance, a litigant has instituted legal action to prevent the publication of certain content that is deemed not to be of public interest, and that all courts of competent jurisdiction dismissed the action. Under this scenario, the litigant would probably be estopped, by virtue of the doctrine of *res judicata*, from instituting new proceedings a later point in time, even ten or twenty years later when the content published is not of public interest anymore.

Second, extinctive prescription or periods of limitations could also raise a significant challenge in a similar context. For instance, in Quebec, the *Civil Code of Quebec* defines “extinctive prescription” as “a means of extinguishing a right owing to its non-use or of pleading a peremptory exception to an action.”²⁸⁶ While the period for extinctive prescription depends on the nature of the action, it generally varies between one and three years with respect to personal rights.²⁸⁷ In common law provinces, various statutes of

284. DONALD J. LANGE, *THE DOCTRINE OF RES JUDICATA IN CANADA* 1 (LexisNexis Canada, 4th ed. 2015).

285. *Id.*

286. *Civil Code of Québec*, S.Q. 1991, c 64, art. 2921 (Can.).

287. *Civil Code of Québec*, S.Q. 1991, c 64, art. 2922 (Can.) states that “[t]he period for extinctive prescription is 10 years, except as otherwise determined by law.” However, with respect to personal rights, Article 2925 provides that “[a]n action to enforce a personal right or movable real right is prescribed by three years, if the prescriptive period is not otherwise determined.” Finally, Article 2929 provides that: “[a]n action for defamation is prescribed by one year from the day on which the defamed person learned

limitations provide for similar principles.²⁸⁸ Therefore, an individual who would like to have certain information published online removed or de-indexed on the grounds that its content is no longer of public interest could find its proceedings challenged on the basis of prescription, if the proceedings are brought more than three years after the initial date of the publication or the date the litigant became aware of the publication.²⁸⁹

These two legal principles may not be well adapted to the increasing availability of digital content. Throughout most of the past century, accessing old content was cumbersome and unwieldy, often requiring access to archives or other databases with limited access. The fact that certain content available to the public was no longer of public interest due to lapse of time rarely had harmful consequences, considering that the content was usually more difficult to access. As discussed under Section 2, over the past years, however, it has become increasingly easy for an individual without research skills to access content that was published five, ten or even fifteen years ago. These legal issues should therefore be addressed in order to ensure that the legal framework can properly address the temporal shift in the availability of digital content online.

2. Decision on Retention and Restoring Data

Quebec courts have been granting 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.²⁹⁰ 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 that had long been forgotten about the plaintiff.²⁹¹ In *Ouellet v. Pigeon*,²⁹² the Court of Quebec held that publishing a descriptive and sensationalist article in the newspaper *Photo-Police* concerning a murder that had taken place ten years earlier (a woman had killed her four children and then committed suicide)

of the defamation.”

288. See, e.g., Ontario Limitations Act, 2002, S.O. 2002, c 24, Sch B (Can.); British Columbia Limitation Act, S.B.C. 2012, c 13 (Can.); Alberta Limitations Act, R.S.A. 2000, c L-12 (Can.).

289. This means that an individual who did not take legal action to prevent the publication of certain content at the time of publication, or within the first three years after they became aware of such publication, would see their recourse prescribed or time-barred, even if the publication is no longer of public interest due to a lapse of time.

290. The legal provision forming the basis of this right is the general extra-contractual civil liability provision found at Civil Code of Québec, S.Q. 1991, c 64, art. 1457 (Can.).

291. This decision was upheld by the Court of Revision. See *Goyette v. Rodier*, [1889] 20 R.L. 108, 110 (Can.).

292. *Ouellet v. Pigeon*, [1997] R.E.J.B. 1997-031906 (Can.).

could not be justified under the public's right to information.²⁹³ The Court ordered the defendant to pay damages to the plaintiff.²⁹⁴

The RTBF assumes that data published becomes less relevant over time and must therefore be deleted at some point. Another aspect to consider when considering the implementation of a RTBF, or any right allowing an individual to request the deletion and/or de-indexation of content published online, is that content that is considered irrelevant (or not of public interest) in the present might become relevant or become of public interest 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. This concern should be considered not only when considering the implementation of a RTBF, but also when considering updating the current legal framework, in order to ensure that there is a legal process allowing for information which becomes of public interest (again) over time to be restored online.

CONCLUSION

The CJEU's landmark ruling in the *Google Spain* case in 2014 sparked a debate on a global scale on the necessity of importing an RTBF. An RTBF would allow individuals to stop data controllers, such as Google and other search engines, 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. European policymakers are also proposing legislation recognizing an RTBF through the Right to Erasure included in the upcoming GDPR.

There is a lack of consensus between the EU and the United States on the legitimacy of this right, which illustrates the cultural transatlantic clash on the issue of the importance of privacy versus other rights, such as freedom of information and freedom of speech. This lack of consensus between jurisdictions is problematic given that it entrains extraterritorial issues. Some EU jurisdiction are requesting that information not only be delisted from European

293. *Id.*

294. *Id.* at ¶ 22 (The Quebec 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").

extensions, but from all extensions, although some are raising that such an extraterritorial effect not only allows someone from a different jurisdiction or country to erase information that they perceive as “irrelevant” or “illegitimate” based on their own set of values; it also arguably promotes one culture’s value of individual privacy rights over other cultures’ value of free expression.

Canada, on the issue of freedom of information and freedom of expression versus privacy, created a balanced legal framework and sits somewhere in between the EU and the United States. Given the broad scope of rights protected by the Canadian Charter and the proportionality test developed by the Supreme Court of Canada in *R. v. Oakes*, the Canadian approach to fundamental rights is more in line with the global (or European) model than the American model, although despite these resemblances With regards to freedom of speech more specifically, the Canadian protection granted to that right appears to be substantially similar to the American one. Canada also adopted data protection laws similar to the European Directive 95/46/EC. The Canadian Charter gives constitutional protection to, *inter alia*, the right to be secure against unreasonable search or seizure, at Section 8, although the Charter does not specifically protect the right to privacy, in contrast to the *Charter of Fundamental Rights of the European Union*²⁹⁵ and the *European Convention on Human Rights*.²⁹⁶

While some ideas inherent to an 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 a European-style RTBF into Canada would most likely prove to be unconstitutional: it may be considered as infringing upon freedom of expression in a way that cannot be demonstrably justified under the Canadian Constitution. Accordingly, any law purporting to create such a right would most probably be struck down by Canadian courts.

Within Canada, Quebec, a primarily French-speaking province, has the most stringent privacy regime and reputational legal framework. The Quebec legal framework addresses some privacy and reputational concerns that an RTBF addresses through the “public interest” test. There are some limits to this framework. The notions of *res judicata* and periods of limitations must be revisited to ensure that this privacy framework can adequately address the fact that with the Internet, data can either outlive the context in which they were published and considered legitimate, or the fact that data that was once considered outdated may become

295. Charter of Fundamental Rights of the European Union, art. 7-8, 2012 O.J. (C 326) 391.

296. EUR. CT. H.R., COUNCIL OF EUROPE, EUROPEAN CONVENTION ON HUMAN RIGHTS, art. 8 (2010).

relevant again and of public interest over time.

Under the Quebec legal framework, courts are charged with arbitrating fundamental rights and values, censorship, availability of historical information, and potential infringements on freedom of expression. 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, with little or no public oversight. Such a secretive process seems poised to favor the removal of information, to the detriment of freedom of expression as these private sector entities will have an incentive to err on the side of removal in order to reduce costs and/or to avoid legal liability and fines to which they could be exposed in case of non-compliance.

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. Efforts should be directed to improving the Canadian legal framework rather than by importing a European-style RTBF that would very likely prove to be unconstitutional and counterproductive.

In the United States, the advocacy group Consumer Watchdog has recently petitioned the Federal Trade Commission to grant every American ‘the right to be forgotten.’²⁹⁷ However, the First Amendment to the United States Constitution seems to clearly overrule any such efforts. The United States Supreme Court, in a unanimous vote, has declared in the 1979 case *Smith v. Daily Mail Publishing Co.*,²⁹⁸ that when a newspaper “lawfully obtains truthful information about a matter of public significance,” it cannot be restricted, “absent a need to further a state interest of the highest order.”²⁹⁹ This principle, set forth in *Daily Mail*, has been specifically applied to search engines, with a court directly declaring that an objection to Google’s search listings methodology is protected by constitutional principles.³⁰⁰ However, given the continued importance of search engine information to public discourse, and the continued debate over the EU efforts to enforce the RTBF globally, challenges based on the RTBF principles are expected in the United States. Although the United States’ standard for free expression protection is broader than that provided in

297. Liza Tucker, *The Right to Bury the (Online) Past*, WASH. POST (Sept. 13, 2015), http://wapo.st/100vOzL?tid=ss_tw [<https://perma.cc/DY8G-Z5W6>].

298. 443 U.S. 97 (1979).

299. *Id.* This case dealt with two newspapers that published articles containing the name of a minor who was arrested for murder. The newspapers were indicted for publishing the name of a juvenile offender, in violation of a West Virginia statute.

300. Jeff Roberts, *Google has Free Speech Right in Search Results, Court Confirms*, GIGAOM, (Nov. 17, 2014, 10:05 AM), <https://gigaom.com/2014/11/17/google-has-free-speech-right-in-search-results-court-confirms/> [<https://perma.cc/C8F6-X32F>].

Canada, Canada's experience in balancing free expression and privacy may be valuable to help assess such future challenges, in the United States, as well as around the world.