



Paying for oblivion: legal and commercial aspects of the right to be forgotten in Canada

RESEARCH REPORT

Report produced by Option consommateurs
and submitted to Innovation, Science and Economic Development Canada - Office of Consumer
Affairs

June 2016

Option consommateurs received funding for this report under Innovation, Science and Economic Development Canada's Program for Non-Profit Consumer and Voluntary Organizations. The opinions expressed in the report are not necessarily those of Industry Canada or of the Government of Canada.

Reproduction of this report, in whole or in part, is permitted provided the source is mentioned. Its reproduction or any reference to its content for advertising purposes or for profit, are strictly prohibited, however.

Written by: Alexandre Plourde

Legal Deposit
Bibliothèque nationale du Québec
National Library of Canada
ISBN 978-2-89716-027-2

Option consommateurs
50, Ste-Catherine Street West, Suite 440
Montréal, Québec
H2X 3V4
Phone: 514 598-7288
Fax: 514 598-8511

Email address: info@option-consommateurs.org
Website: www.option-consommateurs.org

Contents

Option consommateurs.....	iv
Acknowledgments	v
Summary.....	vi
Introduction.....	7
Research Questions.....	7
Methodology.....	8
1. Digital immortality and the right to be forgotten	9
1.1. Infallible, freely accessible memory.....	9
1.2. A few notes on how search engines operate.....	10
1.3. The need to forget and be forgotten	12
1.4. Digital oblivion: a polarized debate	14
1.4.1. Europe: precedence accorded to privacy protection	15
1.4.2. The United States: an attack on freedom of expression	18
2. The policies of search engines.....	20
2.1. A highly concentrated market.....	20
2.2. Similar policies in all jurisdictions	22
2.3. Intermediaries not responsible	24
2.4. A few clearly defined cases	25
2.4.1. Content contrary to policy.....	25
2.4.2. Delisting prescribed by law.....	27
2.4.3. Implementation of the European “right to be forgotten”	29
2.5. Partial transparency	31
2.5.1. Government requests.....	32
2.5.2. Requests under the “right to be forgotten”	33
2.5.3. A call for greater transparency	36
3. Online Reputation Repair Services	38
3.1. Services primarily designed for companies.....	38
3.2. A small, motley industry.....	40
3.3. Cleaning up results pages.....	40
3.4. Outsmarting algorithms: a costly and uncertain exercise	42
4. Canadian law and forgetting	44
4.1. Going to the source.....	44
4.1.1. Removal of personal information.....	44
4.1.2. Defamation and the right to privacy	46
4.2. Delisting publications	49
4.2.1. The “right to be forgotten” from a Canadian perspective	49
4.2.2. Accountability and transparency of Web search services.....	50
4.2.3. Holding algorithms accountable?	52
Conclusion: Towards a Canadian solution.....	55

Option consommateurs

MISSION

Option consommateurs is a not-for-profit organization whose mission is to promote and defend the rights and interests of consumers and ensure that they are respected.

HISTORY

Option consommateurs has been in existence since 1983, when it arose from the Associations coopératives d'économie familiale movement, more specifically, the Montreal ACEF. In 1999 it joined forces with the Association des consommateurs du Québec (ACQ), which had already pursued a similar mission for over 50 years.

PRINCIPAL ACTIVITIES

Option consommateurs helps consumers experiencing difficulties, provides budget consultation and conducts sessions on budgeting, indebtedness, consumer law and the protection of privacy.

Each year we produce research reports on important consumer issues. We also work with policy makers and the media to denounce unacceptable situations. When necessary, we institute class action suits against merchants.

MEMBERSHIP

In its quest to bring about change, Option consommateurs is active on many fronts: conducting research, organizing class action suits, and applying pressure on companies and government authorities. You can help us do more for you by becoming a member of Option consommateurs at www.option-consommateurs.org.

Acknowledgments

This research was conducted and written by Alexandre Plourde, lawyer, under the supervision of Maryse Guénette, head of Research and Representation at Option consommateurs. It was made possible through the financial support of Innovation, Science and Economic Development Canada's Office of Consumer Affairs.

The author wishes to acknowledge the work of all the employees, trainees and volunteers at Option consommateurs who in one way or another collaborated in this research. Particular thanks go to Jonathan Poirier, an intern from Université du Québec à Montréal (UQÀM), for his constant involvement in Option consommateurs' research department. I shall not let be forgotten the contributions of Marie-Claude Juteau and Karim Kimba, paralegal interns from Collège Ahuntsic, Francesca Mihaila, a law student at the University of Sherbrooke, Laurence Laflamme, a law student at the University of Ottawa, Leah Gardner and Pierre-Olivier Valiquette, law students at McGill University, and Emmanuelle Dionne, Sébastien Doyon and Carole-Anne Émond, law students at Université de Montréal. Thank you for giving Option consommateurs the benefit of your talents.

The author also wishes to express his thanks to all those who agreed to grant an interview for this research: Howard Deane, representative of the Consumers Council of Canada, Martin Decelles, search engine optimization expert, Matt Earle, president and founder of Reputation.ca, Jean Goulet, retired Professor from the Faculty of Law, Université Laval, Xavier Manga, co-manager and communications manager at Reputation Net, Jacques St Amant, lecturer in consumer law at UQÀM, Pierre Trudel, Professor at the Public Law Research Centre of the Faculty of Law, Université de Montréal, and Nicolas Vermeys, Professor at the Faculty of Law, Université de Montréal.

Finally, the author extends his gratitude to Bruno Marien, sociologist and lecturer in the Department of Political Science and Law at UQÀM for his methodological support, and to Jean-Pierre Beaud, Dean of the Faculty of Political Science at UQÀM for his evaluation of the report.

Summary

Advances in computer technology have made remembering the norm, and forgetting the exception. Thanks to the networking of information and the ease of access afforded by search engines, anyone can gather a wealth of information about anyone else – instantly. In cases when some of this information is incriminating or obsolete, harm could result to those who are the object of a Web search.

In an attempt to address this problem, the courts of the European Union recently implemented the “right to be forgotten” ruling. This right permits individuals to require search engines not to display a hyperlink to a Website where the information is outdated and is of no public interest. In the U.S., the very broad protection of freedom of expression guaranteed by the Constitution is an obstacle to the development of similar legal solutions.

The policies of the major search engines generally state that they are not responsible for the content of the results pages. It is only in cases of certain specific identifiers or sexually explicit images posted without consent that a hyperlink can be delisted. Search engine operators also claim they comply with laws requiring the removal of content in the countries where they operate. In addition, they offer EU residents a form on which they can make a request under the European “right to be forgotten.” Given the number of requests for delisting they could be faced with, the transparency demonstrated by search engine operators is less than complete.

A few Canadian companies offer online reputation repair services. Their main task is to try to outsmart the algorithms of search engines in order to modify the results pages containing a person’s name. This can be a complex process and one that is expensive for consumers.

Canadian law sometimes offers consumers the opportunity to request companies that store their data to delete it. Canadians also have recourse against publications that illegally violate their privacy or reputation. Although it appears doubtful that Canadian laws on privacy protection can be interpreted in the same way as in Europe, online intermediaries can in certain cases be held liable for illegal content that they disseminate. Finally, deciding just how far search engine services should be held accountable for the results of their algorithms is no easy matter.

The Canadian legal framework does not address all the difficulties raised by Web hypermnnesia, and access to justice is inadequate. However, importing the “right to be forgotten” into Canada is a measure whose efficacy seems limited and threatens the quality of Web search services. The Canadian approach to the issue should be more nuanced, and consider a range of ways of implementing digital oblivion. Search engines should widen the criteria for delisting in their policies in order to tackle situations that have the potential for causing serious harm. However, it is up to Canadian society to democratically determine the limits of forgetting. To achieve this, it seems essential to ensure that the practices of search engine operators are transparent. Finally, part of the solution will also depend on individual behaviour.

Nothing distinguishes memories from other moments. It is only later that they claim remembrance. By their scars.

– Chris Marker, *La jetée* (1962)

Introduction

The Internet is eroding the boundaries between private and public life. Through their posts on social media and their comments on blogs, for example, consumers voluntarily reveal snippets of their private lives. Details about private lives can also be propelled into the public sphere when information about them is reported by the media or migrates to other Websites.

But the Internet never forgets. That youthful error, that unfortunate event or those embarrassing images may be available forever, thanks to search engines. A potential employer or merchant can quickly become aware of a compromising or defamatory item of information about a person... even if it has long been forgotten or forgiven by those concerned.

Within the European Union, the courts have recently implemented a “right to be forgotten” aimed at addressing this problem. This right allows the individual to require search engines not to display hyperlinks to Websites whose information is outdated and of no public interest. On the European version of Google, there is a simple online form to request the withdrawal of search results; thousands of people have already completed the form and many have received a positive response from the company.

Canadian law does not provide similar rights. The solution sometimes offered to Canadians is to pay private companies who promise consumers that, through the use of sophisticated strategies, they are able to manipulate Google search results and reduce the ranking of the most compromising ones and make them “disappear.”

Research Questions

In this research, we studied the means available to Canadians to remove items from the Web and what can be done to better protect them. The permanence of the information stored online coupled with the instant access made possible by search engines give rise to several questions.

What are the practices of the major search engines in Canada? What is the situation in the European Union and the United States? What is the impact on consumers? What paid services are available to Canadian consumers who want to remove such unwanted information? How do these services compare to the right to be forgotten? What are the rights of Canadians affected by harmful information on the Web? Should we be able to remove some of the information from the Web? How can consumers be better protected?

Methodology

In attempting to answer these questions, we first drew up a portrait of the challenges posed by digital immortality and the debate surrounding the right to be forgotten (Section 1). We then analyzed how the most popular search engines in Canada, the U.S. and Europe handle the suppression of hyperlinks (Section 2). We also analyzed the services offered to Canadian consumers who wish to remove information from the Web (Section 3). Finally, we conducted legal research in Canada, the United States and Europe on the right to be forgotten in these jurisdictions (Sections 1.4 and 4).

To aid us in our analysis, we conducted interviews with lawyers involved in privacy protection and with reputed online experts working in various domains. We interviewed Howard Deane, a representative of the Consumers Council of Canada, Martin Decelles, a search engine optimization expert, Matt Earle, president and founder of Reputation.ca, Jean Goulet, retired professor from Laval University's Faculty of Law, Xavier Manga, co-manager and communications manager at Reputation Net, Jacques St Amant, lecturer in Consumer Law at the Université du Québec à Montréal, Pierre Trudel, professor in the public law research Centre, in the Faculty of Law, Université de Montréal, and Nicolas Vermeys, professor in the Faculty of Law, Université de Montréal.

1. Digital immortality and the right to be forgotten

Chris Marker's short film *La Jetée* (1962), dramatizes the predicament of a man whose obsessive memories are so powerful that they open a doorway that allows him to return to the past. In a sense, Marker perhaps was not far from predicting the digital era that was to arrive in the not-so-distant future. In the age of computerization, of rapidly diminishing data storage costs and ease of finding information via search engines, remembering is the norm and forgetting the exception. In this new age, forgetting is a rarer occurrence to which we should never assume we have a right.

1.1. Infallible, freely accessible memory

Only a few decades ago, the most common information storage technologies were forgetful and limited¹. Paper, magnetic tape or vinyl records all degrade over time. Storing information on these media usually involves access to cumbersome technological means, such as a printing press. Since noise is added to each copy of an original, reproduction is imperfect. Also, accessing information stored on analog media can be tedious, and might require long manual searches through sizable archives.

The digital era radically changed this situation. Information is now stored in the form of bytes on computers. These recordings do not degrade, either with time or with use. An indefinite number of copies can be made that are in every respect identical to the original. Digital technology also offers tremendous storage capacity – and this never stops growing. By way of illustration, between 1986 and 2007 worldwide storage capacity increased from 2.5 exabytes to 295 exabytes².

With no memory constraints, computer systems are designed so that, by default, everything gets recorded. In fact, since it requires extra keystrokes in order to erase information, deletion costs usually turn out to be higher than recording costs³. Even if it is removed from one place, the information may often have been replicated somewhere else, which makes it very difficult in practice to permanently erase anything. Unlike human memory, with its built-in forgetting feature, digital memory is infallible.

Digital memory has also become easily accessible through networking. Via the Internet, anyone, anywhere, has access to a mind-boggling quantity of information. The Web is so huge, that it is

¹ The content of this section is largely based on Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, pp. 52-91

² Martin Hilbert and Priscila Lopez, "The World's Technological Capacity to Store, Communicate, and Compute Information" (2011) 332-6025 *Science* 60

³ Colin J. Bennett, Christopher Parsons, Adam Molnar, "Forgetting, Non-Forgetting and Quasi- Forgetting in Social Networking: Canadian Corporate Policy and Practice," in Serge Gutwirth (Ed.), Ronald Leenes (Ed.) and Paul De Hert (Ed.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer Netherlands, 2014, p. 43

practically impossible to measure. According to one estimate, it contains more than four billion Web pages⁴.

However, all this information is completely disorganized. Authors publish on the Internet haphazardly, following no particular logic. Guided only by their whims, they create pages and then insert hyperlinks that link to other pages, to other addresses, and to a wide variety of virtual locations. It thus becomes almost impossible for users to find the most relevant information on the subjects they choose. They need help to make sense of all this scattered information.

Web search engines assume the vital task of organizing the Web⁵. These intermediaries allow anyone, anywhere in the world, to rapidly access the most relevant online information on any given subject. This, incidentally, perfectly echoes Google's declared mission: "to organize the world's information and make it universally accessible and useful"⁶. In this sense, search engines are the true port of entry to the Internet.

1.2. A few notes on how search engines operate

Suppose someone wants to know more about the movie *Solaris*, Tarkovsky's 1972 masterpiece⁷. Like most Canadians, that person will automatically enter the keyword "Solaris" in the query field of a Web search engine. Fractions of a second will be sufficient for a page to appear on the screen showing the most relevant results for that keyword.

On this results page, links to sites (also called "references") will appear in descending order of relevance; the most relevant references will have a "higher" ranking, and the least relevant sites will be pushed further down the page, or assigned to subsequent results pages. These research findings are called "organic," that is to say, they appear on the screen purely because of their relevance to the keywords searched. In contrast, "advertising" results are search results that a company has paid to be displayed, and usually appear in a different form in the results page.

But how, exactly, do search engines manage to deliver these results? Behind the apparent simplicity of the Web search, a sophisticated mechanism is concealed, one that is able to process a stupefying amount of information.

Schematically, the work of a modern search engine is divided into three stages. First, the company explores the Web using computer programs called "crawlers"⁸. These programs have

⁴ This number is quoted from <http://www.worldwideWebsize.com/>. Estimates of the size of the Web can vary greatly from one source to another, some citing figures of up to several tens of billions of pages; here we took the most conservative estimate. For more information on methodological difficulties involved, see: Antal Van Den Bosch, Toine Bogers, Maurice De Kunder, "Estimating search engine index size variability: a 9-year longitudinal study," (2016) 107 (2) *Scientometrics* 839

⁵ James Grimmelman, "The Google Dilemma" (2009) 53 *New York Law School Law Review* 939, pp. 940-941

⁶ <https://www.google.com/about/company/>

⁷ The explanations in this section are largely based on James Grimmelman, "Speech Engines" (2014) 98 *Minn. L. Rev.* 868, pp. 876-879

⁸ At Google, they are called "Googlebots." They are also variously known as "crawlers" or "spiders."

an ambitious mission: to visit billions of Web pages, one after another. To do this, they begin their journey on some of the most important, better-known Websites (e.g. cnn.com) and follow every hyperlink they encounter, on every page they visit.

The company then attributes keywords to each of the billions of pages indexed by its robots – these keywords can be attributed based on the words contained the page itself or on those contained on other pages with hyperlinks that point to it⁹.

These first two steps do not, however, allow a user doing a search to identify the most relevant results of a keyword from all relevant pages. For example, we may have identified all the pages that refer to the term “Solaris,” but no distinction will have been made between those that talk about the original Tarkovsky movie, those that refer to the American remake of that movie, or those that refer to a local solarium manufacturer.

The relevance of these pages is addressed at the third and final stage. To do this, the search engine performs an analysis of the relevant pages based on a set of keywords, using numerous algorithms whose task is to identify pages with a good reputation, of good quality, and that actually deal with the subject that interests the person doing the search.

Search engines naturally do not disclose the exact formulas they use to determine the most relevant results. Their algorithms are trade secrets. Nevertheless, the general criteria used to determine the ranking of a page are quite well known¹⁰. Google says it uses over 200 algorithms simultaneously that are able to analyze various factors such as the number of times the particular keywords appear on a page, where they appear on the page, and whether or not these keywords are synonymous¹¹. Other factors assessed include the page’s browsing history, where it is located, or whether or not the content is new¹². In this analysis process, Google says, the “quality” of a page is accorded priority in determining its relevance¹³.

The best known search algorithm is unquestionably PageRank, which has been developed since the early days of Google¹⁴. Simply stated, this algorithm evaluates the importance of a page by analyzing the links that lead to it together with the quality and popularity of the sites that link to it. The idea behind this method, upon which Google’s success rests, is that quality content will necessarily yield more hyperlinks than mediocre content.

⁹ See: <http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html>

¹⁰ Google publishes a number of documents that contain information about its evaluation criteria and openly advises Webmasters to improve the ranking in which their pages appear. Google Blog: <https://Webmasters.googleblog.com/2015/11/updates-to-our-search-quality-rating.html>. Search Engine Optimization Guide: <http://static.googleusercontent.com/media/www.google.com/en/Webmasters/docs/search-engine-optimization-starter-guide.pdf>. Instructions for evaluators of research quality: <https://static.googleusercontent.com/media/www.google.com/en/insidesearch/howsearchworks/assets/searchqualityevaluatorguidelines.pdf>

¹¹ <http://www.google.com/insidesearch/howsearchworks/crawling-indexing.html>

¹² <http://www.google.com/insidesearch/howsearchworks/algorithms.html>

¹³ See: <http://static.googleusercontent.com/media/www.google.com/en/Webmasters/docs/search-engine-optimization-starter-guide.pdf>

¹⁴ A glimpse of the basic operation of this algorithm is afforded in an article written by Google’s founders. See Sergey Brin and Lawrence Page, “The Anatomy of a Large-Scale Hypertextual Web Search Engine” (1998) 30 *Computer Networks* 107

Search engines are continually perfecting their algorithms, not only to find the most relevant content but also to purge their results pages of what they consider as spam¹⁵. Nor do they really have a choice. A veritable arms race is being waged against certain Webmasters who deploy rather unscrupulous techniques in order to appear among the top search results. For example, since it is known that the number of hyperlinks pointing to a page affects its ranking, Webmasters can create fake Websites containing hyperlinks to pages they want to promote – a technique known as “link farming”¹⁶. They can also manipulate search results using the “Google bombing” technique, which is to associate a specific keyword with a Website by pointing to a multitude of hyperlinks containing the keyword at this site¹⁷.

It goes without saying that search engines excel at the task of organizing the Web. Most of the time, they manage to separate the wheat from the chaff in a Web clogged with poor quality content. Doing a Web search can be helpful in increasing the store of human knowledge... but it sometimes digs up information that is best forgotten, and until recently, would have been.

1.3. The need to forget and be forgotten

Forgetting has an important social and psychological function. The blurring of memories allows individuals to learn from their mistakes without having to forever suffer the consequences. It allows them to act in the present without getting bogged down in details from their past¹⁸. Forgetting gives us the chance to reinvent ourselves, not to be reduced to a single past event, either by ourselves or by others. In society, forgetfulness makes forgiveness possible. It allows wrongdoers to be rehabilitated and an errant citizen’s slate to be wiped clean for the greater good of all¹⁹.

The digital age is upsetting the delicate balance between remembering and forgetting. Certainly, having easy access to an infallible, unlimited collective memory has immense benefits. But the Web’s hypermnnesia could also make forgetting impossible. By simply typing the name of a person into a search engine, large sections of their past can be uncovered at any time. It could dig up articles that would once have been buried in archives, comments posted on social

¹⁵ Google says it has rules that “punish” or accord less emphasis to sites of publishers who try to circumvent its methods of analysis. See: <https://www.google.com/insidesearch/howsearchworks/fighting-spam.html>
<https://support.google.com/Webmasters/answer/35769>

¹⁶ James Grimmelman, “The Google Dilemma” (2009) 53 *New York Law School Law Review* 939, p. 946

¹⁷ The best known case of “Google bombing” is probably the one in which keying in the words “miserable failure” brought up links associated with U.S. President Bush.

¹⁸ For example, Mayer-Schönberger relates the story of a person who had a perfect memory and was able to remember every detail of his life. This had the result of plunging him into a deep state of apathy, preventing him from acting in the present. See Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, 2009, p. 21

¹⁹ For the importance of forgetting for individuals and society, see: Meg Leta Ambrose, Nicole Friess, Jill Van Matre, “Seeking Digital Redemption: The Future of Forgiveness in the Internet Age,” (2012) 29 *Santa Clara Computer and High Technology Law Journal*, Vol. 29, 2012; Maryline Boizard, *Le droit à l’oubli*, Faculté de droit et de science politique, Rennes 1, 2015, p. 8

media²⁰ or information found in a corner of the Web. The bytes will never fade; nor will the memory of the information they carry.

Someone who has lived through a drama, who has committed an error of judgment or has been the target of cruel online criticism may have to bear the stigma forever. Cases can range from trivial to tragic. Someone might see embarrassing pictures of themselves forever linked to their name. Someone else could constantly be reminded of a crime they committed or they were a victim of. Yet another may see an image of themselves downloaded onto the Web without their consent, and posted all over the world²¹. Such people are exposed to people making decisions about them based on information that belongs to the past, whether in the context of a business relationship or employment – without their even knowing. Their social lives can also be affected, for example, when new acquaintances do a Web search on them²². Formerly, you could leave your native village and start life afresh; today, no one escapes the global village.

In Canada and abroad, the right to be forgotten in the digital context has been proposed as a solution to these new challenges²³. In the media, the term “right to be forgotten” is widely used to describe the ability to require the deletion of obsolete links in the results pages of search engines. Conceptually, however, the right to be forgotten extends further than that: it can be defined as a person’s right to request that information about them no longer be released after a certain period of time has elapsed, meaning that its dissemination would no longer be relevant²⁴. The objective of the right to be forgotten is not, in itself, to erase information; information can be “forgotten” simply by being made more difficult to access.

There are in fact many ways of achieving oblivion in the digital context. Of these, the simple deletion of information is the most draconian approach: this involves permanently erasing information hosted online, such as comments published on social media or on Web pages. A less intrusive approach is to make information anonymous, which does not remove the content, but removes or amends the information linking it to a person’s identity. For example, the name of a

²⁰ According to *eMarketer*, there were 20 million users of social media in Canada in 2015: Cindy Liu, *Worldwide Social Network Users: eMarketer’s Updated Estimates for 2015*. In the world, every minute, users publish 2.5 million items of content on Facebook, 300,000 tweets and 220,000 new photos on Instagram. See: <http://aci.info/2014/07/12/the-data-explosion-in-2014-minute-by-minute-infographic/>

²¹ In Canada, one well-known case was that of the “Star Wars Kid,” a teenager whose classmates had posted an embarrassing video of him. See: <http://www.lactualite.com/societe/le-retour-du-star-wars-kid/>

²² In 2010, a study by the Pew Research Center revealed that 27% of adult web users worked for an employer with policies based on how they appeared online. 31% had searched for the name of a colleague or a competitor online, and 16% had done a search online for a person they were acquainted with. See: <http://www.pewinternet.org/2010/05/26/reputation-management-and-social-media>. A 2009 study funded by Microsoft attained similar results: <http://www.microsoft.com/privacy/dpd/research.aspx>

²³ In Canada, the Commissioner for the Office of Privacy Protection has become interested in the debate in recent years: https://www.priv.gc.ca/media/sp-d/2014/sp-d_20140815_pk_e.asp; https://www.priv.gc.ca/media/sp-d/2012/sp-d_20120709_02_e.asp

²⁴ This definition is based on the following sources: A. Cassart and J.-F. Henrotte, *Droit à l’oubli : une réponse à l’hypermnésie numérique*, Droits de l’homme numérique, 56ème conférence de l’IUA, November 1, 2012, p. 4; Saminda Pathmasiri, “L’Internet n’oublie jamais! dit-on. Est-ce toujours vrai?” in *Développements récents en droit du divertissement*, Éditions Y. Blais, 2015, pp. 6-7; Maryline Boizard, *Le droit à l’oubli*, Faculté de droit et de science politique, Rennes 1, 2015, pp. 12-13

person appearing in a newspaper article or on Wikipedia could be removed²⁵. Other options can be imagined, such as programming computer systems to put an expiration date on certain types of data²⁶.

Delisting Web pages is only one of a range of possible ways to promote digital oblivion. Removing an item of information from the results pages of a search engine can, in practice, be a great help in making this information disappear from the collective memory. Even if the original page is still online, access to it is now closed. Technologically, however, delisting is not solely the business of search engines; publishers have control over it too. In fact, Webmasters can delist pages from their Websites by simply inserting a HTML tag header into them that is specifically designed for this purpose.

Figure 1: HTML tag for Web crawlers

```
<meta name="robots" content="noindex">
```

The “noindex” attribute in this HTML tag tells Web crawlers not to index the page. Although robots can choose to ignore this statement, Google says it respects it²⁷.

Of course, despite the multiplicity of methods and actors involved, search engines, due to their crucial role in the dissemination of online information, play a central role in implementing digital forgetting. Although the right to be forgotten relates to far more than the mere possibility of requesting search engines to delist hyperlinks, it is primarily this facet of the right that we focus on in our study. Semantically, it would be more correct here to speak of a “right to delist” when talking of search engines rather than the “right to be forgotten”; unless otherwise stated, we will both use terms interchangeably to describe the consumers’ ability to make search engines “forget.”

1.4. Digital oblivion: a polarized debate

Should forgetting be imposed on search engines? On opposite sides of the Atlantic, this issue is conceived within two very different legal conceptions of the activities of search engines. In Europe, it is considered that a search engine processes personal data when it combines information relating to a person’s name. In the United States, greater emphasis is placed on

²⁵ Meg Leta Ambrose, “You are What Google Says You are: The Right to Be Forgotten and Information Stewardship” (2012) 17 *International Review of Information Ethics* 21, p. 26

²⁶ Saminda Pathmasiri, “L’internet n’oublie jamais! dit-on. Est-ce toujours vrai?” in *Développements récents en droit du divertissement*, Éditions Y. Blais, 2015, pp. 7-11

²⁷ See: <https://support.google.com/Webmasters/answer/93710>

freedom of expression than on protecting the privacy of individuals. In these two legal traditions, the “right to be forgotten” in the digital context has had a very different reception.

1.4.1. Europe: precedence accorded to privacy protection

In Europe, the primary response to the challenges of digital oblivion came from the courts. In 2014, in the case *Google Spain*²⁸ the Court of Justice of the European Union (CJEU)²⁹ issued a liberal interpretation of European standards for the protection of consumer data that allowed Europeans to request that search engines delist certain hyperlinks.

In this case, a real estate agent requested that hyperlinks to pages containing information about seizure for debt, which had appeared online for several years, be removed from Google search results related to his name³⁰. The CJEU upheld the claim by maintaining that Directive 95/46 (The “Data Protection Directive”)³¹, a pan-European legal instrument specifying the obligations for the protection of personal data³², applied to Google search engine activities.

In reaching this conclusion, the CJEU considered that Google, as part of its Internet search business, is responsible for the “processing of personal data” within the meaning of the Directive³³. According to the Court, while performing its automated exploration of the Web, Google collects data, extracts records, organizes and saves them, and communicates them to Web surfers. If the search term is the name of a person, all these actions constitute personal data processing for which Google is responsible because it determines the ends and means.

This entails that, under Directive 95/46, a person may request the deletion of information that is “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed.”³⁴ Plainly stated, a person has

²⁸ *Google Spain SL and Google inc. v. Agenda Española de Protección de Datos (AEPD) and Mario Costeja González*, The Court of Justice of the European Union, May 13, 2014, C-131/12 (hereinafter “*Google Spain*”)

²⁹ The Court of Justice of the European Union (CJEU) is the highest court of the European Union. Its decisions are applicable to all Member States of the European Union.

³⁰ The person also requested the removal of the pages, but this was refused.

³¹ *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal no. L 281 of 23/11/1995, pp. 0031-0050 (hereinafter “Directive 95/46”)

³² The concept of “personal data” covers, pursuant to Art. 2 (a) of Directive 95/46, “any information relating to an identified or identifiable natural person.”

³³ Directive 95/46 applies to anyone “responsible” for the “processing of personal data” (arts. 3 and 4). According to Art. 2 of Directive 95/45, the concept of “processing of personal data” means: “operations which are performed upon personal data, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.” The “controller” is the person who “determines the purposes and means of the processing of personal data.”

³⁴ *Google Spain*, para. 93. Essentially, the CJEU’s reasons are based on several articles of Directive 95/46. Art. 12 (b) provides that a person may ask the controller to rectify or delete their data if its processing does not comply with the Directive, in particular because of the incomplete or inaccurate nature of the data. Art. 14 allows consumers to object to the processing of data relating to them on compelling legitimate grounds relating to their particular situation. Art. 7 (f) states, moreover, that the interests or fundamental rights and freedoms of the data subject may override the legitimate interests pursued by the controller.

the right to request a Web search engine to erase a search result that refers to him that is no longer relevant today – regardless of whether this result causes him prejudice or not³⁵.

One can envisage a situation in which a newspaper article about a person that is posted on the Internet, in perfect compliance with the law, is erased from search results without actually being removed from the Website where it resides³⁶. The delisting obtained by the person only has the effect on search results bearing his name; since the delisted page remains online, it can still be unearthed with a search engine, using keywords other than the person's name. Similarly, the information will still be accessible to anyone who uses the search engine outside the borders of the European Union, whatever keyword is used³⁷.

The CJEU, however, does set a limit on the “right to be forgotten”: the public interest. According to the Court, in each case, a balance needs to be struck between conflicting interests: the right to a person's privacy on the one hand, and the public interest in having access to the information on the other. Most often, according to the Court, the right to privacy should take precedence over the public interest. However, in special cases, the public interest may prevail, depending on the nature and sensitivity of the information or the role played in public life by the person in question³⁸.

The *Google Spain* case, needless to say, complicated the work of search engines operating in Europe. They now had to provide Europeans with a mechanism allowing them to submit requests for delisting in accordance with the “right to be forgotten.” For each request, they had to determine whether a person has the right to be delisted, while attempting to respect the balance between the public interest and the individual's right to privacy. This was certainly enough to give Google employees lots of headaches, especially since the CJEU decision provides little guidance on how companies should go about achieving this delicate balance.

Given the difficulty of the task, two committees developed search engine guidance criteria. In 2014, the Article 29 Data Protection Working Party (A29WP)³⁹, an Advisory Council made up of representatives of agencies for the protection of European privacy, published guidelines for the implementation of the *Google Spain* ruling⁴⁰. In 2015, an ad hoc Advisory Council of experts

³⁵ *Google Spain*, para. 96

³⁶ *Google Spain*, paras. 84-85: The CJEU added that since the processing performed by the search engine is independent of that performed by the publisher, the consumer may apply directly to the search engine to request removal. Similarly, it may well be that, for the same content, posting by the publisher is completely legal and respectful of the Directive, for example if the latter benefits from an exemption related to journalistic purposes (Art. 9) while the processing performed by the search engine does not.

³⁷ Debate on this issue has been contentious. While Google initially wanted to limit delisting to the European versions of its search engine (those using top-level domains such as google.fr or google.de), the European data protection agencies also wanted delisting to apply to the “international” version of the Google search engine, i.e. the top-level domain “.com”. Finally, in 2016, common ground was found: Google would apply delisting on its “.com” version when it detected that a user had accessed it from within the territory of the European Union. See:

<https://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom>

³⁸ *Google Spain*, paras. 81-82

³⁹ “The Article 29 Data Protection Working Party” or A29WP, takes its name from Articles 29 and 30 of Directive 95/46, which constituted it.

⁴⁰ A29WP, *Guidelines on the implementation of the Court of Justice of the European Union judgment on Spain and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario González Costeja*, C-131/12, November 26, 2014 (the “Guidelines”)

formed by Google also made recommendations after conducting a series of consultations in Europe⁴¹.

These two committees came up with fairly similar solutions. According to their findings, in deciding whether to grant a delisting, search engines should weigh criteria such as the person's role in public life, the nature of the information in question, the source of the information and of course, the time elapsed since its publication. For example, when the information relates to a person holding a public office, the public interest will be greater⁴². The same goes for when the disputed information is true and is relevant to matters of public importance⁴³, or comes from a reputable publisher⁴⁴ or concerns a serious crime⁴⁵. Conversely, other factors militate for greater respect for the privacy of individuals. This is the case, for example, with sensitive information about the sex life of a person or on his or her financial situation⁴⁶. The same applies in cases when disseminating the information may harm the person, when the information relates to a victim of a crime or to someone who has committed a minor offence⁴⁷.

As discussed in Section 2.5, Google uses these criteria to assess the requests it receives. Nevertheless, even with the appropriate tagging, the decision-making process involved for the search engines is complex, and contentious situations still emerge. In this regard, it should be noted that Europeans dissatisfied with the decision made by a search engine can appeal to their own country's national data protection agency.

Europe persisted and signed: far from being the sole product of the courts' action, forgetfulness was henceforth enshrined in law with the adoption, in 2016, of the *European Regulation on the Protection of Personal Data*⁴⁸. This regulation, which replaces Directive 95/46, seems to confirm the approach adopted by the CJEU in *Google Spain*. For instance, Article 17 expressly provides for a "right to be forgotten," which entitles individuals to request the deletion of their personal data when they no longer wish it to be processed, "provided there are no legitimate reasons for retaining it"⁴⁹.

⁴¹ Luciano Floridi, Sylvie Kauffmann, Lidia Kolucka-Zuk, Frank Street, José-Luis Pinar Sabine Leutheusser-Schnarrenberger, Peggy Valcke, Jimmy Wales, Eric Schmidt, David C. Drummond, *Final Report of the Advisory Council on Google the right to forgetfulness*, February 6, 2015 (hereinafter "Report of the Google Advisory Council"). This news report at: <https://www.google.com/advisorycouncil/>

⁴² *Report of the Google Advisory Council*, p. 7-8; A29WP, *Guidelines*, pp. 13-14

⁴³ For example, information relating to the political discourse, public health, consumer protection or scientific expression may be relevant to public debate. See: *Report of the Google Advisory Council*, pp. 10-11

⁴⁴ *Report of the Google Advisory Council*, p. 13; A29WP, *Guidelines*, p. 19

⁴⁵ *Ibid.*, pp. 11-12; *Ibid.*, p. 20

⁴⁶ *Ibid.*, pp. 7-8; *Ibid.*, p. 15

⁴⁷ *Ibid.*, pp. 9-10; *Ibid.*, p. 20

⁴⁸ As opposed to directives, regulations apply completely and directly, across all of the EU, without each Member state having to incorporate them in their laws.

⁴⁹ *Regulation (EU) 2016/679 of The European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) COM / 2012/011 final - 2012/0011 (COD)*

1.4.2. The United States: an attack on freedom of expression

In the U.S., the state of the law regarding forgetting is a far cry from what one finds in Europe. The First Amendment of the U.S. Constitution, which protects freedom of expression, has been interpreted very broadly in that country⁵⁰. According to some authors, a company that displays Web search results is exercising its freedom of expression. This affords considerable protection against delisting requests, which could be seen as restricting this freedom⁵¹. In fact, decisions involving Google rendered by U.S. courts reflect this interpretation⁵².

Similarly, U.S. law provides significant immunity to search engine operators with regard to the publications they disseminate. Under section 230 of the *Communications Decency Act*, they cannot be sued for posting illegal content published by third parties on their Websites⁵³. It is those who post the online information who are responsible for it, and even then, although U.S. law provides remedies for obtaining the removal of information affecting a consumer's privacy⁵⁴, the courts have generally accorded enormous protection to freedom of expression and freedom of the press in their decisions⁵⁵.

Nor do our neighbors to the south have any comprehensive legislative framework for the protection of personal information. Some types of personal information may in certain circumstances be protected by special laws. This is the case, for example, for information contained in credit files⁵⁶, the privacy of children online⁵⁷ or, more recently, intimate sexual images broadcast without a person's consent⁵⁸. Since 2015, California law has allowed minors to request webmasters to remove content published on their Websites⁵⁹. However, in the absence

⁵⁰ For example, in 1975 the United States Supreme Court ruled that the publication in the media of the names of rape and murder victims was permitted under the United States Constitution, even though a law of the state of Georgia forbade this, since the Constitution supersedes this law. For other examples, see: Saminda Pathmasiri, "L'internet n'oublie jamais! dit-on. Est-ce toujours vrai?" in *Développements récents en droit du divertissement*, Éditions Y. Blais, 2015, pp. 19-20

⁵¹ Allyson Haynes Stuart, "Google Search Results: Buried if Not Forgotten" (2014) 15-3 *NCJL & Tech.* 463, pp. 487-492; Eugene Volokh and Donald M. Flak, "Google First Amendment Protection for Search Engine Search Results" (2012) 8 *JL Econ. & Pol'y* 883

⁵² *Search King v. Google*, No. CIV-02-1457-M, 2003 WL 21464568 (W.D. Okla. May 27, 2003); *Langdon v. Google, Inc.*, 474 F. Supp. 2d 622 (D. Del. 2007)

⁵³ See, for example: *Zeran v. Am. Online, Inc.*, 129 F.3d 327 (3rd Cir. 1997)

⁵⁴ In the US, there are four torts directly related to the protection of privacy ("privacy wrongs"): Intrusion upon Seclusion, Public Disclosure of a Private Fact, False Light and Appropriation. See: *Restatement (Second) of Torts* §§ 652A-E, <http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html>

⁵⁵ Steven C. Bennett, "The "Right to Be Forgotten": Reconciling EU and U.S. Perspectives" (2012) 30 *Berkeley J. Int'l Law* 161, p. 170-171; Jean Goulet, "Entre la mémoire et l'oubli, le Code civil du Québec et la protection de la vie privée" (2003) 188 *Développements récents en droit de l'accès à l'information* 83, p. 87-88

⁵⁶ *Fair Credit Reporting Act*, 15 USC § 1681. This law requires credit agencies to follow reasonable procedures to protect the confidentiality, accuracy and relevance of personal credit information.

⁵⁷ *Children's Online Privacy Protection Act of 1998*, 15 USC §§ 6501-6506. This Act dictates what a Website must include in its privacy policy and imposes obligations on Webmasters to protect the privacy of children under 13 years of age.

⁵⁸ Several U.S. states have recently adopted "revenge porn laws," i.e. laws that criminalize non-consensual disclosure of intimate sexual images.

⁵⁹ *Privacy Rights for California Minors in the Digital World*, CA Bus & Prof Code §§ 22580-22582

of an American law similar to the EU Directive, the interpretation that search engines essentially process personal information in the course of their activities is out of the question.

It is easy to see that the American legal tradition attaches greater importance to freedom of expression, freedom of the press and the right to information than to protection of privacy. Faithful to this legal tradition, many American commentators have decried the *Google Spain* decision, arguing that it gives individuals the power to censure, or even the ability to remove, segments of history, merely on the pretext that they do not like them⁶⁰. In the context of a democratic society, this not only raises questions about access to information, but also about the role to be played by private companies such as Google in determining what should or should not be available online.

Here in Canada, the question of forgetting raises important issues that also touch on these two divergent approaches to the role of search engines – one based on the protection of privacy, and the other on freedom of expression. In determining where Canadians stand on these issues, we studied the practices of search engines, the commercial options available to consumers for removing information from the Web and their rights in this regard.

⁶⁰ For an overview of these criticisms, see: *Harvard Law Review*: “Google Spain SL v. Agencia Española de Protección de Datos” (2014) 128 *Harv. L. Rev.* 735. Even John Oliver, the famous host of a U.S. late night TV show, made fun of Europe’s “right to be forgotten.” See: <https://www.youtube.com/watch?v=r-ERajkMXw0>

2. The policies of search engines

By opening the doors of knowledge, search engines provide a valuable service to consumers. Sometimes however, they open the doors to a flood of indiscretions. Can these gaps be sealed? How willing are search engine operators to delist hyperlinks? To answer these questions, we analyzed the policies and delisting practices of the largest search engine services in Canada, the United States and the European Union.

2.1. A highly concentrated market

In order to select the most important search engines in each jurisdiction, we used data from StatCounter, which publishes statistics on the market share occupied by the search engines in several countries⁶¹. In each jurisdiction studied, we used data from September 1, 2014 to September 30, 2015⁶².

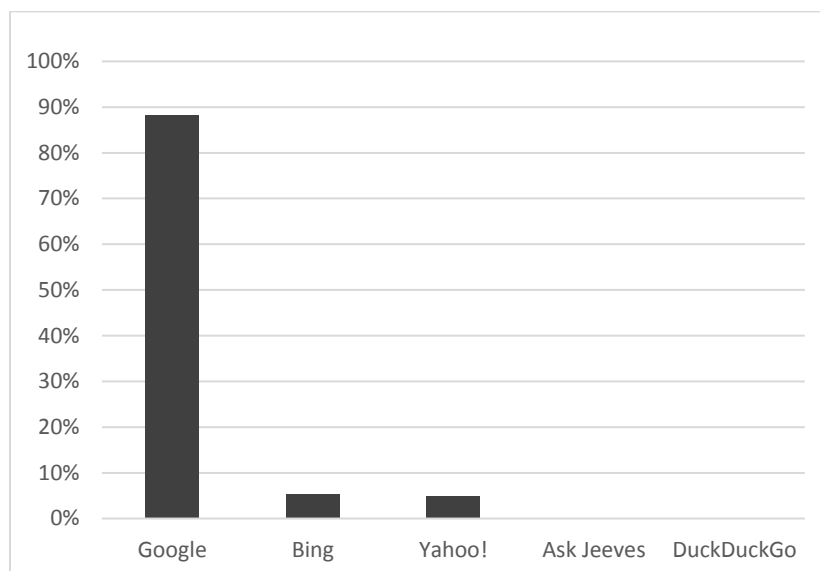
The Web search market is highly concentrated. Google dominates in all the charts; the company has 88.87% of the market in Canada, 80.23% in the United States and 93.43% in France. Besides Google, the only search engines with any significant market share in these jurisdictions are Bing and Yahoo. In total, about 99% of the market is held by three players⁶³.

⁶¹ There are relatively few rankings that compare the importance of search engines in every jurisdiction we studied. Such data is collected by firms such as ComScore, Hitwise, Netmarketshare or Statista, but we were unable to access them free of charge. Data collected by StatCounter Global Stats, which is freely available, enabled us to make comparisons based on the same methodology for all jurisdictions studied. The rankings we arrived at based on this data are quite comparable with the results of other analyses. For example, our results for Canada are consistent with the statistics disclosed by Hitwise, which show that Google, Bing, Yahoo and Ask are the most important search engines in the country, see: <http://www.experian.com/marketing-services/online-trends-canada.html>. In 2012, the Pew Research Center in the U.S. obtained similar results even for the United States, see: Kristen Purcell, Jonna Lee Rainie and Brenner, *Search Engine Use 2012* PewResearchCenter, 2012, p. 9

⁶² StatCounter data can be isolated depending on the type of device that is used to access the internet: “desktop,” “mobile,” “tablet,” or “console.” In collecting the data for our study, we did not discriminate among the different types of devices.

⁶³ The exact percentage of market share of Google, Yahoo and Bing combined is 99.18% for Canada, and 98.47% for the United States. Our data did not give exact percentages for the entire European Union, but the percentage was 99.55% for France.

**Market shares of the five largest search engines in Canada
(September 1, 2014 to September 30, 2015)**



Because of this very high market concentration, we limited our analysis to the five major search engines in each jurisdiction.

For Canada, we selected the following search engines:

CANADA ⁶⁴	
Search engine	Market shares
Google	88.87%
Bing	5.42%
Yahoo	4.89%
Ask	0.21%
DuckDuckGo	0.2%

For the United States, we selected the following search engines:

UNITED STATES ⁶⁵	
Search engine	Market shares
Google	80.23%
Bing	9.2%
Yahoo	9.04%
AOL	0.48%
Ask	0.33%

⁶⁴ Source: http://gs.statcounter.com/#all-search_engine-CA-monthly-201409-201509-bar

⁶⁵ Source: http://gs.statcounter.com/#all-search_engine-US-monthly-201409-201509-bar

It was in the European Union that we experienced the greatest difficulties selecting. Google, Bing and Yahoo are the five most popular search engines in all 28 Member States of the European Union. However, the next most popular search engines differ from one State to another⁶⁶. In order to give a more representative picture of the entire European Union, we have included, in addition to Google, Bing and Yahoo, the two search engines that figured among the top five in the greatest number of States⁶⁷.

EUROPEAN UNION	
Search engine	Many States (28)
Google	28
Bing	28
Yahoo	28
Ask	25
DuckDuckGo	11

Note that this selection corresponds exactly to that of France considered in isolation⁶⁸. For this reason, we focused our analysis on the French versions of these search engines⁶⁹.

2.2. Similar policies in all jurisdictions

For each search engine selected, we analyzed all the documentation available to Internet users in order to locate information relating to their search results delisting policies⁷⁰. This includes these services' conditions of use, privacy policies, user help pages and any other relevant information posted elsewhere on the companies' Websites.

⁶⁶ The most original is the case of the Czech Republic, where 25% of the country's market share is held by the Seznam search engine.

⁶⁷ Of course, this method does not necessarily mean that Ask and DuckDuckGo are the most important search engines after Google, Yahoo and Bing: some search engines that are popular in just a handful of States could still have a greater number of users, in absolute terms, than these two. However, we believe that our selection method permits us to provide an overview of the European Union.

⁶⁸ Market share in France is distributed as follows: Google (93.43%), Yahoo! (3.23%), Bing (2.89%), Ask (0.17%), DuckDuckGo (0.1%)

⁶⁹ Since the *Google Spain* decision on the European "right to be forgotten" applies throughout the European Union, we have not discussed the possibility of changes in the policies of the Member States; moreover, Google says that it does not apply the decision differently in each Member State. The choice of France is also justified because, according to Google's *Transparency Report*, it is the country with the greatest number of requests under the right to be forgotten, <https://www.google.com/transparencyreport/removals/europeprivacy>

⁷⁰ We conducted our analysis between September 1, 2015 and December 31, 2015.

We performed the same analysis in Canada⁷¹, the U.S.⁷² and the European Union⁷³. To ensure that the foreign versions of the sites visited were consistent with what a user located in Europe or the United States would see, we accessed the site using search engines via a virtual private network (VPN)⁷⁴ that simulates a location in these jurisdictions⁷⁵.

From the outset, we found that the policies of the search engines and the details they provide with regard to delisting are not significantly different in Canada, the U.S. and Europe⁷⁶. As discussed in section 2.4.3, the only noticeable difference resides in the European versions of the policies of some search engines, which contain additional entries concerning the “right to be forgotten.” Because of the similarity of this policy to those in other jurisdictions, we will deal with these policies concurrently.

The search engines give little information about their delisting policies. Most often, the most detailed explanations appear in their user help pages. Google’s policy unquestionably has the longest and most detailed explanations. The company not only provides user help pages that explain its practices, but also a support tool for users who want to remove information from

⁷¹ Key documents analyzed for the search engines in Canada. For Google.ca: Terms of Service (<https://www.google.ca/intl/en/policies/terms/regional.html>), Privacy Policy (<https://www.google.ca/intl/en/policies/privacy/>) and several User Help Pages (<https://support.google.com/>), including the “Legal Removal Requests” page (<https://support.google.com/legal/answer/3110420>). For Bing.ca: Microsoft Services Agreement (<http://www.microsoft.com/en-ca/servicesagreement/>), Microsoft’s Privacy Statement (<http://www.microsoft.com/en-ca/privacystatement/default.aspx>) and several User Help Pages (<http://help.bing.microsoft.com/>), including the “How Bing Delivers Search Results” page (<http://help.bing.microsoft.com/#apex/18/en/10016/0>). For Yahoo.ca: the Yahoo Canada Terms of Service (<https://policies.yahoo.com/ca/en/yahoo/terms/utos/index.htm>), Privacy Policy (<https://policies.yahoo.com/ca/en/yahoo/privacy/index.htm>) and several user help pages (<https://ca.help.yahoo.com/>), including “Remove search results from Yahoo Search” (<https://ca.help.yahoo.com/kb/search/learn-article-search-result-removal-sln4530.html>). For Ask.com: the Terms of Service (<http://about.ask.com/terms-of-service/>), Privacy Policy (<http://about.ask.com/privacy-policy>) and the service’s Help Pages (<http://help.ask.com/>). For DuckDuckGo.com, we consulted the Privacy Policy (<https://duckduckgo.com/privacy>).

⁷² U.S. versions of the search engines use the top level domain “.com.” For Google.com, Bing.com, Yahoo.com and Ask.com, we analyzed the equivalent documents to those we identified in Canadian versions of these search engines. Usually they were located at either the same, or very similar, Web addresses. For AOL.com, we consulted the Terms of Service (<http://legal.aol.com/terms-of-service/full-terms/>), Privacy Policy (<http://privacy.aol.com/privacy-policy/>) and the service’s Help Pages (<https://help.aol.com/products/aol-search>).

⁷³ European versions of the search engines use the top-level domains of the country where they offer their services, such as “.fr” for France, “.de” for Germany or “.co.uk.” for the United Kingdom. For our purposes, we consulted the French versions of these sites. For Google.fr, Bing.fr, Yahoo.fr, we analyzed the equivalent documents to those we identified in the Canadian versions of these search engines. Usually, the Web addresses were the same or very similar. Ask.com and DuckDuckGo.com show no version with first-level French domains. The content of these sites in Europe is also similar to that found in Canada.

⁷⁴ A virtual private network, or “VPN”, is a system that remotely creates a direct connection between multiple computers. It can be used to change the apparent IP address of a computer and thus bypass certain location restrictions imposed by a Web site.

⁷⁵ To do this, we used the CyberGhost software. For the United States, we simulated a location in New York. For the European Union, we simulated a location in France.

⁷⁶ Except for some minor differences unrelated to delisting issues, the Google, Yahoo, Bing, AOL, Ask and DuckDuckGo policies for Canada and the United States are identical or nearly so. In Europe, we sometimes observed differences in the ways policies were written, especially in Yahoo and Ask. However, besides additions in Europe relating to the implementation of the “right to be forgotten,” the relevant information with regard to delisting was quite similar from one jurisdiction to another.

search results⁷⁷. This tool, whose tree structure is quite complex, presents the company's policies in question-and-answer format in order to help consumers locate the relevant information and guide them to the forms needed for their requests.

It is the minor players (Ask, AOL and DuckDuckGo) who give out the least information about their delisting practices. Specifically, DuckDuckGo does not address this issue at all in its representations⁷⁸. Given the very modest place these search engines occupy in the market, we can assume that they have not felt the need to publish detailed rules and procedures and are able to handle any requests made to them on a case-by-case basis.

2.3. Intermediaries not responsible

The principle is clear: search engines say they are not responsible for the content of their results pages. They insist that they have no control over the content of the Websites they index⁷⁹. Accordingly, Google repeatedly states that the removal of search results does not remove the content disputed by the consumer:

Google search results are a reflection of the content publicly available on the Web. Search engines can't remove content directly from Websites, so removing search results from Google wouldn't remove the content from the Web.⁸⁰

Bing also states, in the same vein:

Bing doesn't control the operation or design of the indexed Websites, and has no control over what indexed Websites publish. As long as the Website continues to make the information available on the Web and to crawlers, the information will be generally available through Bing or other search engines.

Consequently, since they are not responsible, they invite those who wish to remove content from their results pages to contact the person who does have control, namely the Webmaster:

If you remove content on the Web, you must contact the Webmaster who publishes the data in question. Once it has been removed from the Website and Google has taken into account the update, the information will no longer appear in Google search results.⁸¹

At Google, it seems that trying to contact the person in charge of the site is a precondition for the search engine agreeing to take any action with regard to a listing. For example, Google's support tool asks consumers if they have contacted the Webmaster of the site where the

⁷⁷ See: <https://support.google.com/Websearch/troubleshooter/3111061>

⁷⁸ At most, this search engine invites users to contact the Webmasters of the sites listed: <https://duck.co/help/results/add-or-change-information>

⁷⁹ We found disclaimers of liability for the Google, Bing, Yahoo, Ask and AOL search engines. Most of these companies also invite consumers to contact the Webmasters of the sites referred to withdraw a posting from their results pages.

⁸⁰ <https://www.google.ca/intl/en/policies/faq/>

⁸¹ <https://www.google.ca/intl/en/policies/faq/> <http://help.bing.microsoft.com/#apex/18/fr/10016/0>

information they want to remove is located; if they say no, they are simply directed to a page that gives guidance on how to do this.

2.4. A few clearly defined cases

Although they present themselves as intermediaries not responsible for the content they reference, some search engines say they could, in certain situations, remove links from their results pages.

Google declares that, on its own initiative, it moves quickly to track down and remove certain particularly offensive illegal elements, such as “images depicting sexual abuse of children⁸²”. Similarly, content considered to be “spam” is delisted unceremoniously⁸³; their concern here is with quality of service. More broadly, search engines specifically state that they comply with legal restrictions regarding dissemination and publication that apply in the various countries where they operate, including various forms of restriction on freedom of expression or the development of regional filters for certain types of content⁸⁴.

When they receive a request from individuals to have information about them removed, search engines say that there are two situations in which they act: when this content is not in accordance with their policies (Section 2.4.1), or when it violates the law (Section 2.4.2). In addition, in the Member States of the European Union, some search engines supply a form for submitting a request under the “right to be forgotten” (Section 2.4.3).

2.4.1. Content contrary to policy

The policies of some search engines⁸⁵ specify circumstances in which they may accede to a consumer’s request for delisting. The types of personal information that they are willing to delist however, remain very limited. Essentially, these only cover specific identifiers or situations in which sexually explicit images are posted without the person’s consent.

Google, for instance, agrees to delist pages that contain national identification numbers, bank account numbers, payment card numbers or images of signatures. The “national identification numbers” in question may differ from one country to another. In Canada, it seems that Google

⁸² <https://support.google.com/Websearch/answer/2744324>. Bing, also, goes into some detail about the removal of displayed search results containing or relating to child sexual abuse or the distribution of non-consensual intimate images. Bing says it is cooperating with “credible agencies” to achieve this:

<http://help.bing.microsoft.com/#apex/18/en/10016/0>

⁸³ Google warns Webmasters that it may punish them or delist any content it considers to be spam:

<https://support.google.com/Webmasters/answer/35769>

⁸⁴ For example, Bing said it filters pornographic content in accordance with regional customs and laws; in some states, content labelled “adult” will be subjected to further filtering in search results:

<http://help.bing.microsoft.com/#apex/18/en/10016/0>

⁸⁵ That is to say, the internal rules the company sets itself in managing the content it distributes.

recognizes numbers from only three types of ID: passports, drivers' license and social security numbers⁸⁶. Google justifies delisting these specific items of information by stating that their dissemination "creates significant risks of identity theft, financial fraud, or other specific harms⁸⁷."

According to the company, identifiers of any other type that appear in the search results – such as date of birth, address or phone number – may not be delisted. The same applies to information posted on "official government Websites⁸⁸"; one example would be a government Website that publishes judgments, or another containing information on an individual's criminal history, even if it contains potentially damaging information.

In addition, Google supplies a form to request delisting images of nudity or explicit sexuality that were posted without the consent of the person concerned⁸⁹. This option has likely become available to users as a result of a Google announcement in June 2015 to the effect that it would be providing a procedure to delist content designated by the term "revenge porn"⁹⁰. Google's tree also leads to a form to request the delisting of a "pornographic Website containing the name of a company or the full name of an individual": this option, however, only seems to target situations in which the person's name is associated with pornographic content that is unrelated to that person⁹¹.

Besides Google, other search engines give few details about their delisting policies – and far fewer about their procedures⁹². Yahoo tersely suggests that it can remove some references that contain sensitive information about a person:

If a Website contains Personally Identifiable Information, known as "PII" (like a social security number, or credit card number), then Yahoo may be able to remove the info from our search results, even though we cannot control the Website where it's published.⁹³

⁸⁶ These three types of documents are those that appear in the support tool that Google provides to guide consumers, and exclude any other identification. The consumer is directed to these choices when they click "I want my personal and confidential information removed from Google search results (e.g. social security or national identification number, bank account or credit card number, or an image of your handwritten signature, or a nude or sexually explicit image or video of you that has been shared without your consent)."

⁸⁷ <https://support.google.com/Websearch/answer/2744324>

⁸⁸ <https://support.google.com/Websearch/answer/2744324>

⁸⁹ To get to the form in question, you have to click on the option saying that you want to delete "A picture of me." This option is not intuitive for the user who wishes to request that such content be removed. A help page on this topic would be useful to guide the user through the steps: <https://support.google.com/Websearch/answer/6302812?hl=en>

⁹⁰ "Revenge porn" or "pornographic vengeance" consists of sexually explicit publications that are uploaded without the consent of the person depicted, apparently with a motive of "revenge." See the Google blog post: <https://publicpolicy.googleblog.com/2015/06/revenge-porn-and-search.html>

⁹¹ In the form, Google sets three conditions for delisting: the page must have pornographic content, the name of a person must have been posted without consent, and it must be "spam" according to Google's definition. This last condition seems somewhat contradictory; when a content is considered "spam," Google can delist it on its own, with no other criteria; why then create a specific category for suppressing such situations?

⁹² We found no reference to the removal of such information in the policies of DuckDuckGo, Ask or AOL.

⁹³ <https://ca.help.yahoo.com/kb/search/learn-article-search-result-removal-sln4530.html>

As for Bing, its explanations seem to be contradictory. From the outset, the company invokes the risks to privacy that disseminating certain information may cause:

From time to time, Webpages that are publicly available will intentionally or inadvertently contain sensitive personal information posted without the consent of the individual identified or in circumstances that create security or privacy risks. Examples include inadvertent posting of private records, private phone numbers, identification numbers and the like, or intentionally and maliciously posting email passwords, login credentials, credit card numbers, or other data intended to be used for fraud or hacking.⁹⁴

However, it continues by reiterating that it has no control over such content and invites those involved to contact the relevant Webmasters to have them removed.

We understand that when faced with such requests, search engines have wide discretion to decide what they choose to delist or otherwise. For example, Google says it deals with the situations that are reported to it on a case-by-case basis: “If we believe that a removal request is being used to try and remove other, non-personal information from search results, we will deny the request⁹⁵”.

2.4.2. Delisting prescribed by law

It is not hard to understand that some people might want search results removed for many reasons other than those that the search engines list in their policies. They may feel that certain hyperlinks lead to pages that infringe their reputation or privacy. They may request that the search results be removed simply because they do not like them or because they are outdated.

Search engines deal with such issues in summary fashion: it is up to the law to decide what should be removed or not. Depending on the country, the publication or distribution of online information may be illegal for a variety of reasons: it may, for example, constitute defamatory content, copyright infringement or any other situation in which the state law prohibits dissemination of content such as hate speech or certain types of pornography. Bing, for example, explains:

Certain countries maintain laws or regulations that apply to search service providers and require removal of access to certain indexed pages. Some of these laws allow specific individuals or entities to demand removal of results (such as for copyright infringement, libel, defamation, personally identifiable information, hate speech, or other personal rights), while others are administered and enforced by the government⁹⁶.

Determining whether a publication is illegal is primarily a matter for the courts. An individual who, for one reason or another, obtains a court order requiring a search engine to remove a

⁹⁴ <http://help.bing.microsoft.com/#apex/18/en/10016/0>

⁹⁵ <https://support.google.com/Websearch/answer/2744324>

⁹⁶ <http://help.bing.microsoft.com/#apex/18/fr/10016/0>

hyperlink can obviously compel it to do so⁹⁷. Google also suggests that it can delist publications that are deemed illegal by the courts of a country, even if the judgment contains no prescription directly ordering it to do so⁹⁸. To this end, it even supplies a form to send it judgments “against third parties who have posted allegedly unlawful content.” For example, a person who successfully sues a blogger could transmit the judgment to Google, even if the company is not involved in the court decision.

The Google policy also suggests that it is not always necessary for a judgment to be rendered for the company to believe that a certain content violates the law – and to delist it. For example, someone claiming to have been defamed can fill out a form identifying the disputed URLs and give reasons⁹⁹. A similar form is available to those who wish to challenge Google search predictions that would be “against the law”¹⁰⁰.

Figure 2: Example of Google search predictions



Google search predictions are possible search terms that are added automatically after a user types into the query field.

More specifically, search engines claim that they take action against publications that violate laws respecting intellectual property, and they supply forms for reporting such violations¹⁰¹. Several search engines state that they comply with the *Digital Millennium Copyright Act*, a U.S. law that provides that an undertaking such as a search engine service possesses immunity with respect to references that violate third party copyrights, provided that it removes said

⁹⁷ DuckDuckGo explains it this way: “Also, like anyone else, we will comply with court-ordered legal requests. However, in our case, we don’t expect any because there is nothing useful to give them since we don’t collect any personal information.” See: <https://duckduckgo.com/privacy>

⁹⁸ “I am in possession of a court judgment establishing that certain content has been published illegally (following a lawsuit for infringement of copyright or a trademark, for example)”

⁹⁹ The form asks the consumer to assert his reasons, simply: “Please explain in as much detail as possible what factual statements at this URL you contend are false, or otherwise what it is about the page’s content that is defamatory according to the laws in force in your country.” See: https://support.google.com/legal/contact/lr_legalother?product=Websearch

¹⁰⁰ See: https://support.google.com/legal/contact/lr_legalother?product=searchfeature “Allegedly offensive prediction when typing your query”

¹⁰¹ However, we found no reference to this effect on DuckDuckGo.

references in accordance with a set procedure upon being notified¹⁰². Although this law is enforceable only in the United States, it seems that many search engines have decided to extend the procedures outlined within it to their activities worldwide¹⁰³.

In short, based on the applicable legal framework in each country, search engines consider whether or not they should follow through on a removal request from an individual (we will study the legal remedies offered to Canadian consumers in more detail in section 4). However, actions taken in response to requests from individuals, at least when not supported by a judgment, may not be clear, and we do not know the criteria used for assessing each request.

2.4.3. Implementation of the European “right to be forgotten”

In the jurisdictions studied, the only significant distinction between the delisting policies concerns the European “right to be forgotten” ruling that resulted from the *Google Spain* decision (see Section 1.4.1). In order to implement this right, the Google¹⁰⁴, Yahoo¹⁰⁵ and Bing¹⁰⁶ search engines available within the states of the European Union provide an online form to permit users to apply for delisting. The Ask search engine invites consumers to send a request by mail¹⁰⁷. We could find no information relating to the “right to be forgotten” procedure in DuckDuckGo.

In all, the “right to be forgotten” request forms are rather brief. They ask users to identify themselves, to state the name they wish to have delisted, to provide proof of identity and, of course, to provide Web addresses and the reasons why they wish to obtain delisting¹⁰⁸. The Bing form asks the user additional questions, such as whether the person in question is a public figure or if he or she occupies an important role in the community, such as teacher, priest, police officer or physician¹⁰⁹.

¹⁰² This is the case for Google, Bing and Ask. AOL, for its part, does not explicitly invoke the *Digital Millennium Copyright Act*, but still offers a notification procedure: <http://legal.aol.com/copyright-reporting/>

¹⁰³ A notable exception: Yahoo seems to have different policies for Canada and the United States with regard to intellectual property. In Canada, its procedure does not appear to enable the applicant to obtain delisting automatically; it merely issues a notice to the alleged infringer: <https://policies.yahoo.com/ca/en/yahoo/ip/index.htm>. The procedure offered in the United States suggests that it complies with the requirements of the *Digital Millennium Copyright Act*: <https://policies.yahoo.com/us/en/yahoo/ip/>. This difference can be explained by the different legal frameworks respecting intellectual property in each of these jurisdictions.

¹⁰⁴ https://support.google.com/legal/contact/lr_eudpa?product=Websearch&hl=fr

¹⁰⁵ This form can be accessed by following this link: <http://bit.ly/1I0G5dM>

¹⁰⁶ <https://www.bing.com/Webmaster/tools/eu-privacy-request>

¹⁰⁷ <http://sp.fr.ask.com/fr/docs/legal/privacy.shtml>

¹⁰⁸ Google invites applicants to explain, for each URL, “(1) how the URL in question concerns you (or, if you are sending this form on behalf of a third party, how it concerns him or her); (2) how the URL that appears in the search results is irrelevant, outdated, or otherwise objectionable. Without this information, we will be unable to process your claim.”

¹⁰⁹ <https://www.bing.com/Webmaster/tools/eu-privacy-request>

Google explains that requests are assessed in accordance with the guidelines of the Article 29 Working Group and the steps outlined in the report produced by its Advisory Council in 2015¹¹⁰. Nevertheless, companies have expressed their discomfort at having to find a balance between the right of individuals to privacy and the public's right to have access information, as required by the *Google Spain* decision:

These are difficult judgements and as a private organisation, we may not be in a good position to decide on your case. If you disagree with our decision you can contact your local DPA.¹¹¹

Yahoo states:

The decision of the Court raises particularly complex issues regarding the balance between the right to privacy of an individual and the public's right to information. Our procedures for receiving and examining requests are still being developed, and we are carefully studying the decision of the Court to assess its impact on our business as well as on our users.¹¹²

Given the delicacy of the task and the potentially high volume of requests, the search engines are careful to point out to users that the processing time may be long¹¹³. The procedure does in fact seem tedious and time-consuming. Google explains that its staff assesses each case brought before it. For more complex cases, which it says corresponds to "a little over 30% of requests¹¹⁴", the Google team sends the case to members of management and to the company's lawyers. In certain situations, in addition to accepting or rejecting, Google may also ask the person making the request for more information.

One particular difficulty faced by search engines lies in the fact that the information on which they have to base these complex decisions comes from only one source: the person submitting the removal request. In a letter sent to 29WG, Google says it often has to accept the applicant's allegations as true, even though they may sometimes be false or incomplete¹¹⁵. Google says that some people may fail to mention that an old item has become a subject of public interest once more due to a person's recent actions; others may fail to mention that the person in question occupies an important public role – items that have not yet been considered in the evaluation.

The search engine operators also tell users that they notify the Webmasters of sites that are subject to removal, but that they do not disclose any personal information while doing so.

¹¹⁰ <https://www.google.com/transparencyreport/removals/europeprivacy/fag/> See section 1.4.1 for details on the work of these committees.

¹¹¹ <https://www.google.ca/intl/en-GB/policies/fag/>

¹¹² Yahoo Form: <http://bit.ly/1IOG5dM>

¹¹³ Yahoo explains: "We will then decide whether or not to block the relevant URL or URLs, taking into consideration numerous factors, including the number, nature and complexity of the requests we receive. We appreciate your patience." See: <https://uk.help.yahoo.com/kb/search-for-desktop/d%C3%A9couvrez-les-options-mises-%C3%A0-votre-disposition-sln24378.html>

¹¹⁴ <https://www.google.com/transparencyreport/removals/europeprivacy/fag/>

¹¹⁵ Peter Fleischer, *Questionnaire Addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the "right to be forgotten"*, July 31, 2014. Online at: <http://online.wsj.com/public/resources/documents/google.pdf>

Similarly, their results pages may contain a statement to the effect that the results have been modified in accordance with the European legislation on data protection; this statement must appear on all results pages that bear a person's name, not just the ones that were the subject of a delisting¹¹⁶.

2.5. Partial transparency

If we are to believe their policies, there are many different situations in which search engines may remove hyperlinks from results pages. These include a removal request from someone as a result of sensitive identifiers or sexually explicit images. They can also result from a court order, a copyright infringement, an implementation of the European "right to be forgotten" or the application of a special law of some other State.

Faced with all these opportunities for delisting – "censorship," some might say –, several of the firms studied say they intend to be transparent toward the public. To this end, Google¹¹⁷, Yahoo¹¹⁸, Bing¹¹⁹ and AOL¹²⁰ post what they call "transparency reports" online. These documents give information on the number and types of requests they receive from governments, and provide various other types of data related to the application of national laws¹²¹. Most companies also say they can transmit, in depersonalized form, a copy of each legal request they receive to Lumen, an independent organization whose mission is to collect and analyze complaints and requests for the removal of content published online¹²².

These transparency reports disclose more or less detailed information concerning requests from governments for access to personal information about users of online services, as well as their removal requests¹²³. The Microsoft and Google reports go into more detail. They also contain information about requests from copyright holders and, of course, statistics on requests received through forms to implement the European "right to be forgotten"¹²⁴.

¹¹⁶ Yahoo states as follows: "We may include a notice to users on our search results pages informing them that some results have been blocked pursuant to EU law. We may also notify the operators or webmasters of websites impacted by your request." See: <https://uk.help.yahoo.com/kb/search-for-desktop/d%C3%A9couvrez-les-options-mises-%C3%A0-votre-disposition-sln24378.html>. Google states as follows: "When you search for a name, you may see a notice that says that results may have been modified in accordance with data protection law in Europe. We're showing this notice in Europe when a user searches for most names, not just pages that have been affected by a removal." See: <https://www.google.fr/intl/en/policies/faq/>

¹¹⁷ <https://www.google.com/transparencyreport>

¹¹⁸ <https://transparency.yahoo.com/>

¹¹⁹ The report covers several Microsoft Bing services, but it says most of the removal requests received by Microsoft relate to the Bing search engine: <https://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/>

¹²⁰ The most recent AOL report is at: <http://blog.aol.com/2016/02/08/aol-releases-transparency-report-for-the-second-half-of-2015/>

¹²¹ We found no such reports at DuckDuckGo and Ask.

¹²² This organization was formerly called Chilling Effects. It says it received requests from some of the biggest players on the Web, including Google, Twitter, Wikipedia, WordPress and Reddit. See: <https://www.lumendatabase.org/>

¹²³ Note that the AOL report, which is very brief, gives only a few figures on government requests received. We will not refer further to this document in this research.

¹²⁴ The Google report also provides information on many other aspects that are not relevant here, such as traffic on its products and the detection of malicious sites.

2.5.1. Government requests

Search engines classify court decisions and any requests from government agencies or police forces they receive as “government requests”¹²⁵. Although they do not provide details of each request received, the Google and Microsoft reports do give a few brief examples of notices that they have handled. The founder of one Indian political party was able to obtain the removal of photos of himself that contravened local obscenity laws. In Thailand, pages mocking the King were delisted because they did not conform to that country’s laws on *lèse-majesté* (offending the dignity of the sovereign)¹²⁶.

It is not clear whether court orders brought against a search engine by individuals not in a position of authority in a country are considered to be “government requests.” At Microsoft, the position is that such cases are not included in this category, and that the information collected focused on requests from governmental entities¹²⁷. In contrast, Google and Yahoo seem to put in the same bag requests from individuals, accompanied by a court order, claiming that a certain content is illegal, with all sorts of other types of requests from States seeking to have content removed¹²⁸.

In any event, these so-called “government” requests are relatively few in number¹²⁹. Google states that in the period from January 1, 2015 to June 30, 2015, it received only 3,467 such requests¹³⁰. Google’s data also permits it to isolate government requests classified as “court orders.” In the same period, there were reportedly 199 in the U.S., 326 in the European Union and 23 in Canada¹³¹. Taking into account the total population of each jurisdiction, these

¹²⁵ The motives cited by governments to justify delisting can vary greatly. Among these, “defamation” comes top of the list; as Google says: “From January to June 2015, 31% of government removal requests cited Defamation as a reason for removal, 24% cited Drug Abuse, and 15% cited Privacy and Security.” However, these motives should be interpreted with a certain prudence, since they may be a pretext for state censorship.

¹²⁶ These examples are taken from the Google Transparency Report.

¹²⁷ Microsoft explained in these terms: “We have attempted to include in our numbers all court orders if the demand was brought by a government entity; we did not include court orders that were brought by a private party.” See: <http://www.microsoft.com/about/corporatecitizenship/en-us/transparencyhub/crrr>

¹²⁸ Google explains as follows: “Sometimes we’ll be forwarded government removal requests from users, such as when someone attaches a court order showing certain content to be illegal.” Later, it adds: “We regularly receive requests from courts and government agencies around the world to remove information from Google products. Sometimes we receive court orders that don’t compel Google to take any action. Instead, they are submitted by an individual as support for a removal request.” For Yahoo, see: <https://transparency.yahoo.com/faq>

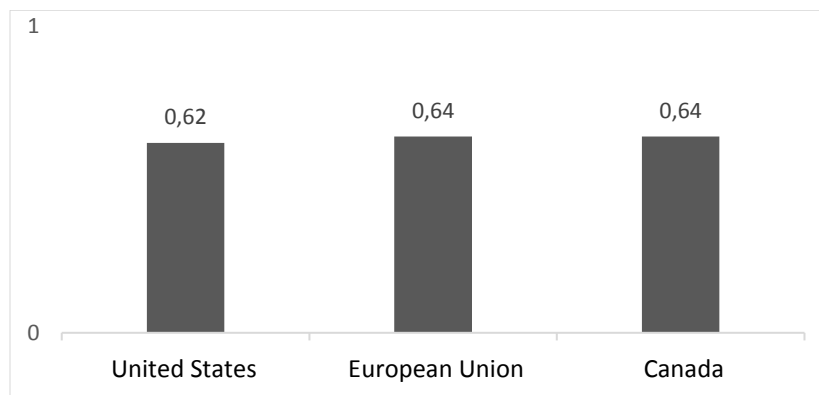
¹²⁹ It will also be understood that a State has other means at its disposal to block content on search engines, for example by blocking the content at the source itself. The removal requests submitted to a search engine do not necessarily represent every case of censorship that takes place worldwide.

¹³⁰ One application may, however, request the removal of multiple items. For example, a request from the British Competition Bureau was for the removal of 93,360 fraudulent ads that redirected users to sites with the motive of defrauding them.

¹³¹ Google does not provide figures for the entire European Union; in establishing the number of “court orders” received in that jurisdiction, we added up the numbers disclosed for each of the EU Member States. Also, Google states that it accedes to these requests in 86% of cases in the U.S. and in 83% of cases in Canada. The only figures we have for the EU are for France (95%).

numbers show that Google received less than one court order per million inhabitants during that period.

**Number of court orders received by Google per million inhabitants
(January 1, 2015 to June 30, 2015)¹³²**



Despite the different legal traditions on opposite sides of the Atlantic, Google's data suggests that, in practice, it does not receive significantly more court orders in any jurisdiction¹³³.

2.5.2. Requests under the "right to be forgotten"

In contrast, far more requests have been made under the European "right to be forgotten" than government requests. In its transparency report, Google states that in the two years since the *Google Spain* ruling came into force (May 2014-May 2016), the company has received more than 400,000 removal requests involving 1.5 million Web addresses. Google agreed to delist approximately 43% of the Web addresses submitted. In comparison, Microsoft reports far less impressive figures for its own search engine Bing: the company claims to have received 3,546

¹³² We obtained these numbers by comparing the number of court orders with the total population of the jurisdiction studied. Demographic data taken from: <http://www.tradingeconomics.com/european-union/population>

¹³³ These results are also similar to those obtained by Jane R. Bambauer and Derek E. Bambauer, who argue that, from 2010 to 2012, the United States actually witnessed a similar number of URL removal requests per million users as in the European Union. See: Jane R. Bambauer and Derek E. Bambauer, *Vanished*, Arizona Legal Studies Discussion Paper No. 13-46, 2013.

requests for the period January to June 2015. Without a doubt, the “right to be forgotten” is primarily a Google affair¹³⁴.

Search engines do not give details about each request received under the “right to be forgotten” or on the decision it made about each of them. However, Google does offer a few (very brief) examples of these that help clarify how it applies the European decision¹³⁵. Moreover, since the implementation of *Google Spain*, the media has also reported a number of cases of delisting, thus shedding some additional light on the situation¹³⁶.

As far as we can ascertain, the examples of delisting decisions taken by Google are generally in line with the principles laid down by its Advisory Council and 29WG (Section 1.4.1). Victims of crime, such as rape victims or the widow of a man who was murdered, have been able to obtain the removal of links to media articles that cited their names. The removal of links to pages reporting criminal acts was also obtained when the crimes involved were minor or happened long ago, or had since been pardoned. People were also able to get links to pages removed that contained information related to their health, that contained a photo of them posted without their consent¹³⁷, that recalled events they had been involved in as minors¹³⁸ or simply contained their address¹³⁹.

Google did, however, reject some other claims. This was the case with professionals who had committed crimes or mistakes in the course of their work¹⁴⁰. The same applied to requests regarding the antics of people occupying important public roles; for example, a high-ranking official was denied delisting of recent articles recalling a criminal conviction that occurred ten years ago¹⁴¹. The gravity of the crime is also an important factor; for example, a removal request from a priest convicted for possession of child pornography was refused. Cases arising from situations in which the applicants had themselves disseminated undesirable content were also

¹³⁴ It is worth mentioning that these numbers still seem quite modest compared to the hundreds of millions of removal requests submitted annually by copyright holders. In fact, in February 2016, Google received requests to delist more than 76 million URLs. In such cases, Google claims that it acceded to 97% of requests submitted to it. See: <https://www.google.com/transparencyreport/removals/europeprivacy/fag>; <http://variety.com/2016/digital/news/google-dmca-copyright-removal-requests-piracy-1201740892/>. This high level of delisting is probably explained by the American legal process with respect to copyright, which is based on the “notice and takedown” model.

¹³⁵ We found no information on the specific cases at Microsoft.

¹³⁶ For example:

http://www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html

¹³⁷ Google case “An individual asked us to remove a link to a page that had taken a self-published image and reposted it. The page has been removed from search results for her name.”

¹³⁸ Google case “An individual asked us to remove a link to an article covering a contest in which he participated as a minor. We have removed the page from search results for his name.”

¹³⁹ Google case “A woman requested that we remove pages from search results showing her address. We have removed the pages from search results for her name”

¹⁴⁰ Google case “One individual asked us to remove 20 links to recent articles about his arrest for financial crimes committed in a professional capacity. We did not remove the pages from search results. We also refused an individual’s request to remove 2 links to articles covering an investigation of sexual abuse accusations while in his professional capacity.”

¹⁴¹ Google case “A prominent business person asked us to remove articles about his lawsuit against a newspaper. We did not remove the articles from search results.”

rejected¹⁴².

Some cases reported in the media involved more complex situations that demonstrate the delicacy of the task of search engines in implementing the *Google Spain* decision. One person who injured a passenger when driving his vehicle while drunk was able to obtain a delisting¹⁴³. Another, who had been acquitted of a violent crime due to a mental disorder, was unable to do so¹⁴⁴. Someone who was acquitted of a serious crime committed during the last five years was able to obtain a delisting¹⁴⁵. Someone else, however, was denied a request to have pages delisted that referred to a trial in which they were acquitted, since the case was still recent¹⁴⁶.

Although Google rejects the majority of requests to have offending links removed, few consumers appear to have appealed its decisions to any of the 28 national privacy protection agencies in the European Union – even though they have the right to do so. According to journalist Peter Teffer, who investigated the situation, no more than 2% of those who received such a refusal file a complaint with these agencies¹⁴⁷. France's Commission Nationale de l'Informatique et des Libertés states in its 2015 annual report that it had received nearly 700 complaints in this regard since the *Google Spain* decision came into force, 45% of which were legitimate¹⁴⁸.

Finally, search engines do not release comprehensive information on the reasons given by consumers for their "right to be forgotten" requests. However, statistics on the types of cases submitted to Google have reached the media through informal channels¹⁴⁹. Similarly, Reputation VIP, a company that provides an automated support service to anyone wishing to make a request under the "right to be forgotten" via the Forget.me Website, has also published data on cases processed¹⁵⁰.

¹⁴² Google case "A media professional requested that we remove 4 links to articles reporting on embarrassing content he posted on the Internet."

¹⁴³ <http://www.economist.com/news/international/21621804-google-grapples-consequences-controversial-ruling-boundary-between>

¹⁴⁴ <http://www.economist.com/news/international/21621804-google-grapples-consequences-controversial-ruling-boundary-between>

¹⁴⁵ Google case: "An individual who was convicted of a serious crime in the last five years but whose conviction was quashed on appeal asked us to remove an article about the incident. We removed the page from search results for the individual's name."

¹⁴⁶ <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion>

¹⁴⁷ <https://euobserver.com/investigations/130590>

¹⁴⁸ <http://techno.lapresse.ca/nouvelles/internet/201603/24/01-4964195-google-prie-dappliquer-uniformement-le-droit-a-loubli-en-europe.php>. Courts have rendered some decisions with regard to delisting all over Europe. See Stefan Kulk and Frederik Zuiderveen Borgesius, "Freedom of Expression and 'right to be forgotten' cases in the Netherlands after *Google Spain*" (2015) 2 *European Data Protection Law Review* 113; Noémie Lepot, *Le droit à l'oubli numérique au sein de l'Union européenne : consécutions actuelles, lacunes et perspectives futures*, Master's thesis conducted under the direction of Madame Andrée Puttemans, professor at the Free University of Brussels, 2015, p. 30. In one of these decisions, a French woman was able to get articles delisted that referred to criminal conviction that occurred eight years previously. See: *TGI DE PARIS, Ordonnance de Référé du 19 DECEMBRE 2014 Marie-France M. / Google France et Google Inc.* http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4425

¹⁴⁹ <https://www.theguardian.com/technology/2015/jul/14/googles-data-leak-right-to-be-forgotten>

¹⁵⁰ <http://www.reputationvip.com/blog/right-to-be-forgotten-statistics-and-key-dates>

According to these sources, which need to be treated with caution given their informal nature, the majority of removal requests are from ordinary individuals who want links to personal information online to be removed¹⁵¹. Reputation VIP places 58.7% of requests into the “Invasion of Privacy” category, which covers a variety of cases including disclosure of a private address or a religious or political opinion displayed against one’s will¹⁵². Next, at 11.2%, is the “Defamation and Insult” category, which includes cases of defamation. “Damage to Image” accounts for 4%; “Homonyms” for 1% and “Death” for 0.7%¹⁵³. Although Google’s transparency report and the media often highlight examples of delisting related to criminal cases, cases involving “Criminal procedure” or “Presumption of Innocence” only account for 5% of requests submitted in Forget.me¹⁵⁴.

According to Reputation VIP, the most common grounds for a search engine refusing to remove a link are when the information concerns the person’s professional life (26%), when the person is the originator of the content (22%) or when the information is still relevant and in the public interest (14%). In 13% of cases, requests would be refused due to the fact that they relate to the social network profile of the person making the request – it seems that some consumers are poorly informed about the possibility of removing information from their social media accounts and ways of adjusting privacy settings.

The main targets of delisting are social networks (20%), directories and content aggregators (14.8%) and blogs (4%)¹⁵⁵. This confirms Google’s assertion in its transparency report to the effect that Facebook is the site that is the subject of the largest number of removal requests. News sites account for 3.3% of requests and Wikipedia, 0.2%¹⁵⁶.

2.5.3. A call for greater transparency

Whether in relation to government requests, the “right to be forgotten” or other types of requests, the transparency of the search engine providers is unfortunately only partial. The information disclosed clearly does not cover every case of removal request that a search engine might receive. While the policies of search engines raise the possibility of removing hyperlinks containing certain identifiers or pornographic images that could be detrimental to the person portrayed, their transparency reports have nothing to say on these issues.

Similarly, search engines are still unclear about the types of cases submitted to them and their responses to them. We do not know what answers are given to consumers who allege that information disseminated by a search engine is illegal – for example, because it is defamatory – but have not obtained a judgment to support their claims¹⁵⁷. Similarly, we can only form an idea

¹⁵¹ <https://www.theguardian.com/technology/2015/jul/14/googles-data-leak-right-to-be-forgotten>

¹⁵² <http://www.reputationvip.com/blog/right-to-be-forgotten-statistics-and-key-dates>

¹⁵³ Cases classified under “Other” totaled 16.9%

¹⁵⁴ The same can be inferred from Google’s data: <http://syttp.github.io/rtbf/index.html>

¹⁵⁵ <http://www.reputationvip.com/blog/right-to-be-forgotten-statistics-and-key-dates>

¹⁵⁶ The Wikimedia Foundation also maintains a page listing notices it receives to delist articles: https://wikimediafoundation.org/wiki/Notices_received_from_search_engines

¹⁵⁷ The Lumen database was of little use, as all we usually found there was metadata that is difficult to combine for analytical purposes.

of the implementation of the “right to be forgotten” through a few very brief examples and through informal channels; essentially, the types of cases submitted and the decisions made are beyond the public eye. This opacity has been deplored by several privacy protection experts around the world, who in 2015 signed an open letter to Google demanding more transparency with regard to its “right to be forgotten” practices¹⁵⁸.

¹⁵⁸ <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.jy4fwk3ab>

3. Online Reputation Repair Services

Like it or not, the hypermnnesia and ubiquity of the Web can have a considerable impact on the importance of our online image. Some experts even believe that the information found on the Internet about someone – their online profile – will soon be as important as their credit rating¹⁵⁹. In fact, the content of search engines' results pages can be used as the basis for many decisions on consumers – often without their knowledge.

There are several things people can do to take care of their online image. For example, they can go online and create profiles on social media or set up a blog, where they can publish content that highlights their interests and ideas¹⁶⁰. Additionally, either for free or for a low fee, there are applications such as BrandYourself¹⁶¹, Trackur¹⁶² or Google Alerts¹⁶³ that enable consumers to monitor what is said about them on the Internet, analyze these comments, and respond quickly if necessary.

But sometimes these inexpensive aids are not enough. Consumers in Canada who are targeted by negative publications, either in the media or online, can see their reputation seriously tainted when doing a Web search for their name. As we have seen, it is only in a few select cases that search engines will accede to a removal request. Furthermore, undertaking legal proceedings to get certain publications removed can be long and costly. So what can be done?

With the burgeoning growth of the Internet, a veritable industry has been born that offers online reputation repair services. These Web arrangers come under a variety of labels: they claim to offer “online reputation management” or “search engine optimization” or “online identity management”¹⁶⁴. In French, the most commonly used terms are “réputation en ligne,” “e-reputation” or “déréférencement.” All these epithets come down to one and the same thing: the ability to control one's image online and ultimately thwart the algorithms of search engines to make them forget some unwanted hyperlinks. In short, paying for oblivion.

3.1. Services primarily designed for companies

In our study, we wanted to know more about the services offered by such companies in Canada. To do so, we conducted a comprehensive keyword search¹⁶⁵ and obtained a list of Websites of

¹⁵⁹ That at least is the opinion of Tom Bryce, founder of the U.S. company Metal Rabbit Media. See:

<http://bits.blogs.nytimes.com/2011/04/04/the-growing-business-of-online-reputation-management/>

¹⁶⁰ <http://www.theguardian.com/technology/2013/may/24/search-me-online-reputation-management>

¹⁶¹ <http://brandyourself.com/>

¹⁶² <http://www.trackur.com/>

¹⁶³ <https://www.google.ca/alerts>

¹⁶⁴ Other expressions may be used, including: “Search Engine Reputation Management,” “Internet Reputation Management,” “Search Engine Deoptimization” or “Google Washing.”

¹⁶⁵ We used keywords that a consumer seeking information on reputation services online would use intuitively, in both English and French. Google Searches were conducted on the following expressions: “online reputation Canada,” “online reputation,” “e-reputation,” “personal online reputation Canada,” “nettoyage réputation numérique,” “réputation en ligne,” “réputation en ligne Canada,” “déréférencement,” “déréférencement Canada,” “déréférencement Québec,” “déréférencement Québec agence”, “agence marketing Canada réputation en ligne,”

companies in Canada that offer services to consumers that claim to enhance their online reputation¹⁶⁶. In the absence of reliable data on the online reputation industry in Canada¹⁶⁷, this selection method has enabled us to draw up a representative picture of the consumer's point of view.

Our search turned up a total of 41 firms that have a place of business in Canada. However, we found that the representations of the majority of these firms are addressed solely to companies that want to enhance their online image¹⁶⁸. Only a few of the representations are aimed at consumers, and none of them claims to offer services exclusively tailored to this type of client.

This first finding is hardly surprising. As journalist Isabelle Ducas reports, it is mainly corporations that use online reputation management services; they are concerned that a negative image may affect their sales and are willing to pay on the nail to ensure that adverse comments about their products and services do not appear among the top search results¹⁶⁹.

In our analysis, we restricted our selection to companies that explicitly state that they provide services to individuals¹⁷⁰. Of the 41 companies initially identified, only ten met this criterion: ClickTecs¹⁷¹, E-reputation management¹⁷², Numero Uno¹⁷³, Media Optimization¹⁷⁴, Platina IT¹⁷⁵,

"agence marketing Québec réputation en ligne," "agence marketing e-reputation Canada," "suppression de lien moteur de recherche," "suppression de lien moteur de recherche Canada," "suppression de lien moteur de recherche Québec," "suppression résultat recherche Google," "suppression résultat recherche Google Canada," "suppression résultat recherche Google Québec." For each search query, we combed through the sites appearing in the top 100 results. In many cases, the same companies come up in these search queries.

¹⁶⁶ To find out if the company had a place of business in Canada in determining the type of services offered, we relied on the information on the company Website.

¹⁶⁷ We did not find any data providing giving an overview of the online reputation market in Canada. A study by the Consumers Council of Canada in 2011 conducted an analysis of ten online reputation firms in Canada, but the selection of companies was not based on data compiled by other organizations. See Howard Deane, *Canadian Consumers: Online Reputations, Awareness, Misuse and Repair*, Consumers Council of Canada, 2011, p. 65. A French study of 2010, which was interested in this market in France, referred on a list of e-reputation agencies created by a blogger: <https://cadderep.hypotheses.org/agences-en-e-reputation>. See: Peggy Cadel, "Le marché de l'e-réputation. Du positionnement fonctionnel aux enjeux technologiques," *Les Cahiers du numérique* 2010/4 (Vol. 6) pp. 111-121. In the U.S., we found several rankings for the "best" companies in the sector. See, for example: <http://www.10bestseo.com/agencies/reputation-management/>. For Canada, however, we found no lists similar to those identified in France and the United States. In addition, during our research, we estimated that the results of our keyword Internet search permitted us to obtain a more representative picture of what average consumers themselves could find on the Web when searching for this type of company.

¹⁶⁸ We visited all the sites of these companies to determine which representations were addressed.

¹⁶⁹ Isabelle Ducas, "Profession: redresseur de réputation," *La Presse*, September 29, 2013; see also: Karim Benessaïeh, "Conseils de pros," *La Presse*, June 4, 2015

¹⁷⁰ It is not impossible that firms excluded from our selection offer services to consumers, without mentioning this on their Websites. However, we believe that our approach has produced information that is pertinent from the perspective of consumers, who do not have access to other sources of information when selecting the company they deal with.

¹⁷¹ <http://clicktecs.com/>

¹⁷² <https://www.martindecelles.com/e-reputation-management-montreal/>

¹⁷³ <http://www.numerounoWeb.com/>

¹⁷⁴ <https://www.optimizationmedia.com/online-reputation-management-orm/>

¹⁷⁵ <http://www.platinait.com/remove-negative-reviews/>

Reputation.ca¹⁷⁶, Net Reputation¹⁷⁷, Reverse SEO¹⁷⁸, Vortex Solution¹⁷⁹, Web and Candy¹⁸⁰. We analyzed the service offering of these ten companies in detail by browsing their Websites. Also, three representatives of these companies – Martin Decelles, search engine optimization expert, Matt Earle, president and founder of Reputation.ca and Xavier Manga, co-manager and communications manager at Réputation Net – agreed to answer our questions.

3.2. A small, motley industry

The companies we studied wear a variety of hats. Although some firms, such as Reputation.ca or Reputation Net, specialize solely in online reputation management¹⁸¹, the others come from the communications or Web design sectors; online reputation services forming only part of their broader service offering¹⁸².

Companies that are exclusively dedicated to online reputation management are small. By way of illustration, Matt Earle says his company, Reputation.ca, with its 14 employees, is probably the largest of its kind in Canada. The company E-reputation management is operated entirely by its owner, Martin Decelles. This means that the online reputation management market for individual consumers in Canada is still very small.

According to Mr. Earle, the industry is more firmly established in the United States. Companies such as Reputation.com, BrandYourself, ReputationX or InternetReputation.com have dozens, even hundreds of employees¹⁸³. According to Mr. Earle, the strength of the U.S. industry is explained in part by the fact that U.S. laws are less protective of privacy than Canada's.

3.3. Cleaning up results pages

The descriptions of the services offered by the firms we studied are short and very similar¹⁸⁴. Essentially, they explain that their services are designed to downgrade the rank of unwanted hyperlinks on results pages linked to an individual's name:

¹⁷⁶ <https://www.reputation.ca/>

¹⁷⁷ <http://reputationnet.net>

¹⁷⁸ <http://reverseseo.ca/>

¹⁷⁹ <http://www.vortexsolution.com>

¹⁸⁰ <https://www.Webcandy.ca/>

¹⁸¹ The firms that correspond to this definition are: E-reputation management, Reputation.ca, Reputation Net, and Reverse SEO

¹⁸² This phenomenon of mixed genres also seems not to be unique to Canada; the e-reputation market in France also appears to be heterogeneous in character. Peggy Cadel, "Le marché de l'e-réputation. Du positionnement fonctionnel aux enjeux technologiques," *Les Cahiers du numérique* 2010/4 (Vol. 6), p. 112

¹⁸³ For example, in 2014, Reputation.com announced it had hired 150 people:

<http://www.azcentral.com/story/money/business/2014/06/25/reputationcom-opening-tempe-office-hire/11363557/>

¹⁸⁴ Besides the general representations on their sites, most of these companies include a promotional blog or publish articles that provide more information on their services; these include: ClickTecs, E-Reputation Management, Reputation.ca, Numero Uno, Reverse SEO, Reputation Net. Some publish videos: Reputation.ca, Numero Uno, Reverse SEO.

With the help of online reputation management, you can manage the results that search engines and social media sites display to people when they search for your brand or name. With effective online reputation management, you can boost your positive aspects and eliminate or conceal the negative ones.¹⁸⁵

The most commonly accepted strategy for doing this is to publish and promote content that shows the person in a favorable light, then index it with the use of search engines. This could involve writing and distributing positive posts about the client online, launching a Website to showcase these publications, publishing articles on Wikipedia, writing comments on blogs – as well as creating hyperlinks to these publications, to give them importance in the eyes of search engine algorithms. One company explained this as follows:

In concrete terms, we put emphasis on creating pages and messages on various Websites, social network platforms and blogs, in order for them to appear at the top on search engine results, thus eliminating all negative content¹⁸⁶.

In addition to creating or enhancing positive content in order to “drown out” unwanted content, some companies argue that they are able to erase posts put out by certain defamatory sites¹⁸⁷. Reputation.ca, for example, states:

Our experts are able to completely remove defamatory posts on ComplaintsBoard.com, TheDirty.com, Globe24H.com, Cheaterville.com, and many similar defamation Websites. We can also successfully remove negative posts about you from social networks, forums, message boards and other online liabilities.¹⁸⁸

Reputation Net says it will attempt to obtain the removal of unwanted comments by contacting the host and settling the problem amicably:

If all conditions are met, an amicable negotiation with the host will remove the offending link. This involves sending the host a digital and/or physical message clearly indicating links to content that infringes on your reputation that you wish to delete. The goal is to obtain this deletion as soon as possible, relying on the good faith of the host¹⁸⁹.

However, this approach is not always advisable. According to experts, sending a judicial request to the author or host of undesirable content could have the effect of drawing attention to the issue in question, which could lead to increased traffic and even spawn new, undesirable posts. Generally, the experts maintain that confrontation is to be avoided: attempting to retort to the author of malicious online content can often exacerbate the problem.

¹⁸⁵ <http://www.numerounoWeb.com/online-reputation-management/>

¹⁸⁶ <http://www.vortexsolution.com/dereferencement.html>

¹⁸⁷ We found claims like these at: Reputation.ca, Reverse SEO Optimization Media, Reputation Net

¹⁸⁸ <https://www.reputation.ca/personal/>

¹⁸⁹ <http://reputationnet.net/?p=346> [translation – English version unavailable on site]

Thus, among the companies studied, only Reputation Net raises the possibility of taking legal action to remove Web content. The firm, however, makes it clear that “since every case is different, the choice of a simple de-indexation, or the use of content flooding may be preferred following a pre-intervention diagnosis¹⁹⁰”.

Finally, prevention is always better than a cure. Several firms offer services for keeping an eye on one’s online reputation. For example, consumers can verify what is being said about them online by being given access to interfaces or warning systems. Reputation.ca, for example, offers a service that provides consumers with a daily report on their situation.

3.4. Outsmarting algorithms: a costly and uncertain exercise

In the eyes of search engine operators, exploiting the criteria of their algorithms to influence the results pages is not in itself an unfair practice. In its blog for Webmasters, Google itself invites people wanting to disappear from search results to create new publications online:

Instead, you can try to reduce its visibility in the search results by proactively publishing useful, positive information about yourself or your business. If you can get stuff that you want people to see to outperform the stuff you don’t want them to see, you’ll be able to reduce the amount of harm that that negative or embarrassing content can do to your reputation.¹⁹¹

But in many cases, replacing unwanted content is a challenge. As mentioned in Section 1.2, the algorithms of search engines are very sophisticated and are being perfected constantly. In determining the most relevant results for a keyword in a search, they are not limited to listing the pages and hyperlinks that point to them: they are interested in the quality and importance of the pages, and display admirable sleuthing ability in detecting false or misleading content.

As a result, the experts we interviewed do not recommend the use of tricks such as drafting bogus content, astroturfing¹⁹² or link farming¹⁹³. Purchasing keywords for advertising purposes is not a solution because it has no influence on organic search results. In sum, there is no shortcut for cleaning up an online reputation: Web users have to confine themselves to creating and distributing truthful, original Web content of good quality.

And to do things properly, you have to be prepared to loosen your purse strings. Among the experts interviewed, suggested prices ranged from \$500 to \$6,000 per month, depending on the services rendered and the difficulty of the case. Among the sites studied, only one – Reputation.ca – announces the price of its services¹⁹⁴. The company offers a service to change

¹⁹⁰ <http://reputationnet.net/?p=346>

¹⁹¹ <https://googleWebmastercentral.blogspot.ca/2009/10/managing-your-reputation-through-search.html>

¹⁹² Astroturfing is using a pseudonym or a false identity in one’s online interactions. See: Geneviève Grenier, *Bloggers or Floggers?: Undercover advertising exposed*, Research report by Option consommateurs submitted to Industry Canada’s Office of Consumer Affairs in 2012

¹⁹³ “Link farms” are fake sites that allow networks to create multiple hyperlinks to lure search engines toward content they want to promote. See: Section 1.2

¹⁹⁴ <https://www.reputation.ca/pricing/>

the results pages of search engines at a basic cost of \$3,000, plus \$2,500 per month. For deleting information from some sites, price ranges from \$499 to \$10,000. Given that several months' work may be needed to achieve visible results, hiring serious companies to manage one's online reputation can incur significant expense for the average consumer.

According to the experts interviewed, the clients that appeal to their services are mostly quite wealthy or already enjoy a certain reputation: professionals, public figures and politicians. According to Matt Earle, the people who use his services often have a financial interest in their online image. Average consumers, on the other hand, will contact him primarily in regard to major problems; this could be the case, for example, with parents whose children have been exposed online.

Even if one pays a high price, using the services of an online reputation firm does not guarantee that the search results about a person can actually be changed. Outsmarting algorithms is complex – and the more a person's online reputation is tainted, the more difficult it is to drown out undesirable posts among other, more positive ones. In some cases, especially for people with a known criminal past or who have been in the centre of major controversies, the task seems so onerous that some firms refuse them¹⁹⁵. In fact, it seems that in many cases a person's online reputation is a fairly accurate reflection of their "offline" reputation; accordingly, despite the digital age, it is still a good idea to build up a good reputation in the physical universe.

¹⁹⁵ Companies also refuse clients for ethical reasons. Both Mr. Earle and Mr. Decelles say they have refused to provide services to individuals wishing to hide serious crimes, including crimes related to child abuse.

4. Canadian law and forgetting

Strictly speaking, there is no “right to be forgotten” in Canada. However, Canadian law sometimes offers consumers the opportunity to request the deletion of personal information from companies who hold it (Section 4.1.1). Consumers can also challenge publications that illegally infringe their privacy or reputation (Section 4.1.2). Although it appears doubtful that Canadian laws can be interpreted in the same way as European laws (Section 4.2.1), online intermediaries can sometimes be held liable for the illegal content they disseminate (Section 4.2.2). Finally, consideration needs to be given to the accountability and transparency of search engines with regard to their algorithms and practices in the context of digital oblivion (Section 4.2.3).

4.1. Going to the source

The first step in attempting to remove information from the Web is to go directly to the source, either by contacting the organizations that host the data, or the authors of the undesirable posts themselves. The simplest case is when it is the party who makes the request who posted the information they want erased, on social media, for example. In this case, this data could be considered by Canadian law as personal information, and as such, consumers can sometimes obtain a deletion. Moreover, in certain circumstances, consumers can enforce their rights against those who harmed their reputation or assert their right to respect for privacy.

4.1.1. Removal of personal information

In Canada, a company that collects, uses or discloses personal information in the course of its commercial activities must comply with the obligations of the *Personal Information Protection and Electronic Documents Act* (hereinafter the “Federal Act”) or to those of an equivalent provincial legislation¹⁹⁶.

These laws do not explicitly provide consumers with a “right of removal.”¹⁹⁷ However, they do require companies to obtain the person’s consent to process their personal information; it also

¹⁹⁶ S. 26 (2) b) of the Federal Act allows the federal government to exclude its application within the borders of a province that has adopted a law that is “substantially similar” to it, with the exception of “federal undertakings” and the collection, use or disclosure of personal information outside the province for which federal law continues to be applied. Three Canadian provinces have adopted similar laws, that is to say, which contain obligations similar to those contained in the Federal Law: Québec, with its *Act Respecting the Protection of Personal Information in the Private Sector*, RSQ, P-39.1 (hereinafter the “Québec Act”); Alberta, with its *Freedom of Information Protection of Privacy Act*, SA 2003, P-6.5 (hereinafter “Alberta Act”); British Columbia, with its *Personal Information Protection Act*, SBC 2003, 63 (hereinafter “British Columbia Act”). Similarly, three other provinces have adopted substantially similar laws, but these only apply to health information custodians: Ontario, with its *Personal Health Access and Protection Act*, 2004, SO 2004, c.3 sched. A; New Brunswick, with its *Personal Health Information Privacy and Access Act*, SNB. 2009, P-7.05; Newfoundland and Labrador, with its *Personal Health Information Act*, SNL 2008, P-7.01.

¹⁹⁷ In Quebec, article 40 of the Civil code states that a person, in a file concerning him, may cause information which is contained in a file concerning him, the deletion of obsolete information or information not justified by the purpose of the file. This article can be added to the protections provided in the Québec Act, in the sense that the right of a person to erase personal information is more explicit.

includes the ability to withdraw such consent¹⁹⁸. Further, these laws require companies to use the personal information they hold only for the purposes for which they were collected¹⁹⁹. These provisions have been interpreted by the Office of the Privacy Commissioner of Canada (OPC) as offering consumers the opportunity to request the removal of data they have created online, and more particularly, what they post on the Internet²⁰⁰. For example, in two of its findings involving social media, the OPC considered that such companies should offer their users viable options for removing their accounts²⁰¹.

The Federal Act has also been invoked in respect of information that was not published by the person concerned. In its findings, the OPC considered that the site Globe24h, which published judgments involving Canadians and made them freely available through the search engines without the consent of the persons concerned, thereby communicated personal information illegally²⁰². However, the company refused to follow the OPC's recommendations²⁰³.

In short, the privacy laws do give consumers some control over their data, including the ability to have it erased. This option may provide a remedy for people who regret the content of their past comments or wish to erase incriminating photos they have posted online. If these postings been indexed by the search engines, their removal will also entail their disappearance from the results pages.

However, there are exceptions. First, Canadian privacy laws do not apply to media that report facts about a person; these exceptions are made for journalistic reasons in order to protect freedom of the press²⁰⁴. Similarly, these laws do not apply to people who handle personal information other than in the course of commercial activities, such as someone who publishes information about a person on their personal Website, from which they derive no financial

¹⁹⁸ See, for example: Federal Act, principle 4.3; Alberta Act, ss. 7-10; British Columbia Act, ss. 6-9. S. 12 of the Québec Act provides that the use of information contained in a file is permitted, once the purpose of file is completed, with the consent of the person concerned.

¹⁹⁹ The Federal Act states that an organization may use personal information only for the purposes for which it was collected and it can keep "as long as necessary for the fulfillment of those purposes" (Principle 4.5). It also states that a company should "destroy, erase or render anonymous personal information that is no longer needed for an identified purpose" (Principle 4.5.3). See also the Québec Act, s. 11; Alberta Act, s. 16; British Columbia Act, s. 14

²⁰⁰ This at least is what the OPC suggests in its guidelines on consent, which state that data specific to the online environment can, depending on the context, be considered to be personal information; this includes "data from social networks created by the user, such as comments, evaluations, "likes" and "dislikes," "Twitter stream." See: https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_f.asp. See also: Colin J. Bennett, Christopher Parsons, Adam Molnar, "Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice," in Serge Gutwirth (Ed.), Ronald Leenes (Ed.) and Paul De Hert (Ed.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer Netherlands, 2014, p. 44.

²⁰¹ *Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act by Elizabeth Denham, Assistant Privacy Commissioner of Canada, Case Summary under PIPEDA No. 2009-008, July 16, 2009 (OPC), paras. 228-256; Nexopia, a social networking site for youth, contravened the Canadian law respecting protection of personal information, PIPEDA Report of Findings, No. 2012-001, section 5*

²⁰² *A revenue-generating Website that publishes Canadian judgments, which by allowing them to be indexed by search engines, contravened PIPEDA. PIPEDA Report of Findings No. 2015-002.*

²⁰³ The OPC says it filed a motion before the Federal Court to decide the issue. See: OPC, *Online Reputation - What are they Saying About Me?*, Discussion Paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada. January 2016, p. 7

²⁰⁴ Federal Act, s. 4 (2); Québec Act, s. 1; Alberta Act, s. 4 (3) c); British Columbia Act, s. 3 (2) b)

benefit²⁰⁵. Finally, these laws may sometimes be impossible to apply to companies located outside the country²⁰⁶.

In practice, moreover, consumers who avail of themselves of the deletion options offered by technology companies are faced with a sizable difficulty: that of knowing whether their wishes are scrupulously observed. A study by Colin J. Bennett reveals that, for various reasons, ranging from protection of their interests to jurisdictional disputes between Canada and the United States, several important social media companies always retain in their archives part of the data that users have asked to be deleted²⁰⁷. According to Mr. Bennett, the deletion options offered by social media are still less than perfect: “few social networking services guarantee that data will, certifiably, be deleted and tend to offer either broad exceptions under which data will be retained or state outright that it will not be deleted.”²⁰⁸

Recently, the Ashley Madison case, in which some remorseless pirates publicized personal information about the users of a highly sensitive site, provided an eloquent illustration of the risks posed by the incomplete removal of consumer data. In this case, some of the users who saw their personal information exposed had already paid the company to make sure their profile had been cleared²⁰⁹. To better protect consumers, we should therefore wish for better monitoring of corporate practices regarding the disposal of personal information.

4.1.2. Defamation and the right to privacy

In addition to their rights with regard to the protection of personal information, Canadians have other rights when they challenge the source of online content.

First, several Canadian provinces protect the right to privacy. Special laws are in force in Saskatchewan²¹⁰, Manitoba²¹¹, BC²¹² and Newfoundland and Labrador²¹³. The Ontario courts

²⁰⁵ Federal Act, s. 4. The Québec Act (s. 1) applies to the processing of personal information in the course of operating a business. The Alberta Act (s. 4 (3) a) and the British Columbia Act (s. 3 (2) a)) state that they do not apply to the collection, use or disclosure of personal information for personal or domestic purposes.

²⁰⁶ The OPC says it has difficulty asserting jurisdiction over foreign sites where there is no substantial connection between the Website and Canada. See: OPC, *Online Reputation - What Are They Saying About Me?*, Discussion Paper prepared by the Policy and Research Group of the Office of the Privacy Commissioner of Canada., 2016, p. 7. In *Douez v. Facebook, Inc.*, 2015 BCCA 279, the British Columbia Court of Appeal ruled that the domicile clause forced consumers to institute proceedings against Facebook in the United States. This case was nevertheless brought before the Supreme Court of Canada.

²⁰⁷ Colin J. Bennett, Christopher Parsons, Adam Molnar, “Forgetting, Non-Forgetting and Quasi-Forgetting in Social Networking: Canadian Policy and Corporate Practice,” in Serge Gutwirth (Ed.), Ronald Leenes (Ed.) and Paul De Hert (Ed.), *Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges*, Springer Netherlands, 2014 pp. 50-51

²⁰⁸ *Ibid.* p. 50

²⁰⁹ <http://www.nytimes.com/2015/08/20/technology/the-ashley-madison-data-dump-explained.html>

²¹⁰ *The Privacy Act*, RSS, c. 24

²¹¹ *The Privacy Act*, CCSM P125. Also, in order to combat “revenge porn,” Manitoba recently passed a law that prohibits the distribution of an intimate image of a person without that person’s consent. See: *Intimate Image Protection Act*, CCSM . 42

²¹² *Privacy Act*, RSBC 1996, c. 373

²¹³ *An Act Respecting the Protection of Personal Privacy*, RSNL1990 c. P-22

have recently recognized a tort on the protection of privacy²¹⁴. In Québec, the right to respect for privacy is enshrined in the *Charter of Rights and Freedoms* and the *Civil Code of Québec*, which explicitly cite examples of invasion of privacy, such as the use of the name or image of someone for any purpose other than the legitimate information of the public²¹⁵.

The laws of the provinces also protect citizens against defamation, that is, damaging their reputation²¹⁶. Defamation is not conceived in exactly the same way in Québec's civil law as in common law²¹⁷. In the common law provinces, a statement can be considered defamatory only if it is false; when the potentially damaging information is accurate, it may be considered an invasion of privacy²¹⁸. In Québec, defamation may not only consist in the intentional dissemination of false information about a person, but also making true, yet unfavourable statements about a person without just cause to do so²¹⁹.

These rights can sometimes provide Canadians with recourse against Internet users who spread gossip and slurs about them, or expose facts about their personal lives or post their image on the Internet without a valid reason. These rights, however, are not absolute. Comments posted on the Internet that affect the privacy or reputation of a person are not automatically illegal for that reason alone. Their publication may be justified because of other rights and interests, such as freedom of expression and the public's right to information²²⁰.

At the center of this complex balance of rights and freedoms, the notion of public interest plays the role of arbitrator. Disseminating information that violates the privacy or reputation of a person may be lawful if it is in the public interest that it be known. Drawing the line is not always easy. According to the Supreme Court of Canada, what is in the public interest depends on the

²¹⁴ *Jones v. Tsige*, 2012 ONCA 32. In this case, the Ontario Court of Appeal recognized the tort of "intrusion on seclusion" which is a deliberate intrusion into someone's private life that would be considered highly offensive to a reasonable person.

²¹⁵ Québec's *Charter of Human Rights and Freedoms*, RSQ, . 12, s. 5; *Code Civil du Québec*, art. 35-41. For further developments on image rights in Québec, see: Geneviève Grenier and Nicolas Sapp, "Le droit à l'image et à la vie privée à l'ère des nouvelles technologies," (2009) 314 *Développements récents en droit de la propriété intellectuelle* 379

²¹⁶ Barry Gamache defines defamation as follows: "It is basically the harm caused to the reputation of a person, for example, through speech or writing. Defamation has the effect of tainting the esteem a person has gained as a result of their social interactions. In case law, defamation essentially consists in the communication of spoken or written words, or even pictures or gestures that lower someone's esteem or consideration in the eyes of others, or that prompt adverse or unpleasant feelings towards them." [translation] See: Barry Gamache, "La diffamation en ligne: ce qu'il ne faut pas mettre sur un blogue," in *Développements récents en droit de la propriété intellectuelle*, Barreau du Québec - Service de la formation continue, 2013, p. 130

²¹⁷ The provincial legal system is not the same in Québec as in the rest of Canada. In Québec, the current system is civil law, based on the French tradition, while in the other provinces it is common law, based on the English tradition. For more information, see: <http://www.justice.gc.ca/fra/sjc-csj/just/03.html>

²¹⁸ *Grant v. Torstar Corp.*, [2009] 3 SCR 640, at para. 59; OPC, *Online Reputation: What Are They Saying About Me?*, Working Paper prepared by the Policy Group and Research of the Commissioner for the Protection of Privacy in Canada, 2016, p. 11

²¹⁹ *Prud'homme v. Prud'homme*, [2002] 4 SCR 663, at para. 35-36; *Amin v. Journal de Montreal*, 2015 QCCQ 5799. Recourse against defamation in Québec is based on civil liability, which requires proof of fault, injury and a causal link (*Civil Code du Québec*, art. 1457). Rather than the veracity of the comments, the criterion of evaluation consists in whether the conduct was at fault and whether it caused injury to the person.

²²⁰ For example, s. 9.1 of the Québec *Charter* states that the fundamental rights and freedoms are exercised with "a proper regard for democratic values, public order and the general well-being of the citizens of Québec."

context, the nature of the information concerned and the situation of the person involved²²¹. Accordingly, it may be of public interest to know certain things about the personal life of an individual with a considerable reputation. The same applies to unknown individuals who suddenly become involved in an activity that is of public interest, such as a lawsuit or an event affecting public safety. Similarly, people who choose to expose themselves in public situations, such as demonstrations or sporting events, cannot expect absolute respect for their privacy.

In Québec, the courts have occasionally acknowledged that remarks made in the media were not of public interest because they unnecessarily brought up past events. In 1986, for example, a court ruled that the *Photo-Police* newspaper had unnecessarily dug up the past by publishing an article about a horrible tragedy that took place many years earlier²²². However, the courts refused the request of another individual whose escapades were still relevant²²³ and another who had chosen to expose himself in a public assembly²²⁴. As Pierre Trudel explains²²⁵, a form of the “right to be forgotten” already exists indirectly in our laws, to the extent that it may be an offence to dig up unsavoury facts about someone’s past²²⁶.

In sum, to say that under Canadian law, consumers will just have to put up with the Web’s inability to forget would be going too far. They do retain some control over their own publications, and in many cases can take them off the platforms on which they appear (see Section 4.1.1). They can also challenge in court certain information published about them that is not in the public interest. For example, slanderous statements or unjustified indiscretions against them may, in theory, be expunged from the Web by instituting proceedings directly against the person who posted them²²⁷.

In practice, however, the legal route is ill-suited to the virtual context. It hardly needs to be pointed out that the difficulties of access to justice for consumers are numerous. Too often, asserting one’s rights is a long, expensive, complex affair²²⁸. On the other hand, posting illegal remarks on the Internet is fast, free and is disseminated very efficiently. The damage will have been done long before the courts arrive at a decision.

²²¹ *Aubry v. Éditions Vice-Versa inc.*, [1998] 1 SCR 591, at para. 57-59; *Grant v. Torstar Corp.*, [2009] 3 SCR 640, at para. 105

²²² *Ouellet v. Pigeon*, REJB 1997-03106, 1997 (CQ). In 1889, Québec courts were faced with a similar case: *Goyette v. Rodier* (1889) 20 RL 108,110 (Rev. C)

²²³ *Lévesque v. Québecor communications inc.*, [1999] RRA 681

²²⁴ *Mathieu v. Presse Ltée (La)*, (CQ, 1998-11-24), NO. 500-02-031538-965

²²⁵ Pierre Trudel is a professor at the Public Law Research Centre (CRDP) of the Faculty of Law of Université de Montréal.

²²⁶ The examples given in this paragraph are taken from Mr. Trudel’s blog:

<http://www.journaldemontreal.com/2014/10/24/le-droit-a-loubli-nest-pas-ne-dhier>. See also: Jean Goulet, “Entre la mémoire et l’oubli, le Code civil du Québec et la protection de la vie privée” (2003) 188 *Développements récents en droit de l’accès à l’information* 83

²²⁷ For instance, in *Laforest v. Collins*, 2012 QCCS 3078, the Québec Superior Court ordered a person who, via a blog, posted remarks on the Internet that were defamatory and prejudicial to another person, to remove said content. The court also required the defendant to provide a retraction letter that could be used to prevent a recurrence of the offending content on the Internet.

²²⁸ See, for example: Comité d’action sur l’accès à la justice en matière civile et familiale, *L’accès à la justice en matière civile et familiale*, October 2013

Similarly, taking legal action can paradoxically increase the damage a person incurs, because of the publicity a trial can generate – what some commentators call the “Streisand Effect”²²⁹. Experts in online reputation, moreover, do not recommend judicializing such problems, and suggest less ostentatious methods for getting stuff to disappear from the Web (see Section 3). Consequently, beyond the changes to our laws, an important part of the reflections on digital oblivion in Canada should be focussed on creating simple, innovative mechanisms for promoting access to justice in the virtual context.

4.2. Delisting publications

By law, the remedies available to consumers first of all target the authors of online publications. But in some cases, even though it seems uncertain that the European “right to be forgotten” can be applied to Canada, it is sometimes possible for online intermediaries, including search engines, to be held responsible for any illegal content they disseminate.

4.2.1. The “right to be forgotten” from a Canadian perspective

Could the European “right to be forgotten” be adopted as it stands in Canada? In Europe, as we have seen, the legal basis for the right to oblivion consists in the consumer’s right to control personal information (see Section 1.4). According to the CJEU, hyperlinks containing the name of a person displayed on a search results page may constitute “personal data” within the meaning of Directive 95/46. Such an interpretation would permit the application of European data protection standards to Google’s search activities.

Although Canadian privacy legislation is based on the same principles as the European data protection standards²³⁰, it is uncertain that such an interpretation could be repeated in Canada. We have seen our laws applied to every organization that collects, uses or discloses personal information in the course of its commercial activities (Section 4.1.1). Certainly, one can easily argue that Web search services such as Google, Bing and Yahoo conduct commercial activities, given the advertising revenue they derive from what they do²³¹. Moreover, in Canada, the notion of “personal information” has been given a very broad interpretation, encompassing a wide range of information or data concerning an identifiable individual²³². However, it is uncertain that the activities of a company that searches and indexes the Web, then produces hyperlinks in response to search queries by users, is subject to Canadian laws on the protection of personal information.

²²⁹ Taking its name from an anecdote about Barbra Streisand, this “effect” describes the phenomenon whereby a person seeking to hide or censor information ends up unwittingly helping make this information better known.

²³⁰ Many privacy laws around the world are based on guidelines developed by the OECD. See: *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. Note that the term “personal data” used in Europe, is replaced by “personal information” in Canada.

²³¹ S. 2 of the Federal Act defines these activities as “any regular course of conduct that is of a commercial character.”

²³² For example, the notion of personal information can broadly include digital traces and data produced by a user. See: Alexander Plourde, *How Free is “Free”? Setting limits on the collection of personal information for online behavioural advertising*, Report submitted to Industry Canada’s Office of Consumer Affairs by Option consommateurs, 2015, pp. 38-40

As a matter of course, the Canadian Constitution is very protective of freedom of expression, and can invalidate any law that unreasonably conflicts with it²³³. This has already occurred in the context of privacy protection. In 2013, the Supreme Court of Canada struck down the *Personal Information Protection Act*, Alberta's provincial law on the protection of personal information, considering that it interfered disproportionately with the freedom of expression of a union in preventing videos and photos to be taken of people who crossed a picket line²³⁴. In its decision, the Supreme Court maintained that the Alberta legislation restricted the collection, use and disclosure of personal information "without regard for the nature of the personal information, the purpose for which it is collected, used or disclosed, and the situational context for that information"²³⁵. This decision leaves uncertainties about the balance to be struck between expressive activities that are published online – as well as the dissemination of these publications via search engines – and a possible individual right, based on the principle of control over personal information, which would allow a person to obtain a delisting of a search engine without necessarily having to suffer harm as a consequence of the information being made public.

This suggests that the design of Canadian laws, based as they are on principles established in the 1980s, may not be adapted to providing solutions in the current technological context. For example, the Federal Act provides for exceptions for "journalistic, artistic or literary purposes"²³⁶, but contains no mention of activities within a technological context such as a Web search. Accordingly, it is uncertain that the legal approach adopted in Europe to confer upon consumers a right to be forgotten by search engines – namely applying personal information protection standards to Web search activities – could work under current Canadian law.

4.2.2. Accountability and transparency of Web search services

While it is uncertain that Canadians will be able to invoke privacy laws against search engine providers in the same way as in Europe, they are not completely defenceless against online intermediaries who broadcast information about them. However, it is only in cases when a publication is illegal – for example because it is defamatory or violates their privacy without cause (see Section 4.1.2) – that they can sometimes hold online intermediaries responsible.

²³³ *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, 1982 [Schedule B to the *Canada Act* 1982, 1982, c. 11 (UK)], ss. 1 and 2 b). The test for determining whether a law is a justified restriction on the Charter was established in *R. v. Oakes*, 1986 1 SCR 103

²³⁴ *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401*, 2013 SCC 62

²³⁵ *Ibid.* para. 25

²³⁶ Federal Act, s. 4 (2) c)

As in the United States²³⁷, Canadian law limits the liability of Web search services with regard to the content of the Websites referred to in their results pages²³⁸. In Québec, the *Act to Establish a Legal Framework for Information Technology*²³⁹ provides that a Web search service, as an intermediary, shall be liable for an unlawful hyperlink that appears in its results pages if it knows about it and does not promptly make the user aware of its existence²⁴⁰. By law, Web search services are not presumed to know about the illegal content they index because they are under no legal obligation to monitor the information they transmit²⁴¹.

Courts in common law jurisdictions have applied a variety of legal solutions. In *Crookes v. Newton*, the Supreme Court of Canada ruled that a person who only makes a hyperlink to a page that contains defamatory statements, without controlling or approving of these, cannot be held responsible for it²⁴². In *Weaver v. Corcoran*, the Supreme Court of British Columbia found that the *National Post* was not responsible for defamatory comments posted by users of its site to the extent that it had no knowledge of these comments, and had acted immediately when they were brought to its attention²⁴³.

These decisions suggest that in common law, a search engine that only provides hyperlinks to defamatory content cannot be held responsible, insofar as it has no control over this; however, online intermediaries could be held responsible for defamatory content whose dissemination

²³⁷ As discussed in Section 1.4.2, s. 230 of the *Communications Decency Act* states that an online intermediary cannot be sued for posting illegal content published by third parties. In Europe, there is a directive that provides for limitation of the liability of intermediaries: *Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market*, Official Journal L 178, 17/07/2000.

²³⁸ Note that in matters of copyright, the obligations of the search engines may be different than those stated here. For instance, the *Copyright Act* states that a search engine service that is notified of a copyright infringement does not have to delist a content, but simply notify the offending party. However, in practice, we have seen that all the search engines except Yahoo, even those in Canada, follow the American procedure prescribed by the *Digital Millennium Copyright Act*, which stipulates that the search engine should remove automatic content that a person claims infringes their copyright, and must give a right of appeal to the person who is the subject of the delisting. See: *Copyright Act*, RSC (1985), ch. C-42, s. 41.25-41.27; Nicolas Vermeys, “C-11, la Loi concernant le cadre juridique des technologies de l’information et la responsabilité des intermédiaires techniques québécois : une dualité de régimes (in)utile(s) ?” (2013) 25-3 *Cahiers de propriété intellectuelle* 1051, pp. 1096-1097. In any event, this aspect will not be discussed in more detail, because it only incidentally concerns consumers wishing to remove online posts about themselves.

²³⁹ RSQ, C-1.1

²⁴⁰ *An Act to Establish a Legal Framework for Information Technology*, RSQ, c. C-1.1, s. 22; Nicolas Vermeys, “C-11, la Loi concernant le cadre juridique des technologies de l’information et la responsabilité des intermédiaires techniques québécois : une dualité de régimes (in)utile(s) ?” (2013) 25-3 *Cahiers de propriété intellectuelle* 1051, pp. 1090-1095. Note that the Québec courts have often failed to mention the *Act to Establish a Legal Framework for Information Technology* in decisions in which it might be applicable. Despite this, their conclusions are nonetheless in line with the principle of limited liability of technical intermediaries stated therein. See: *Canoë inc. v. Corriveau*, 2012 QCCA 109. In *Prud’homme v. Rawdon (Municipality)*, 2010 QCCA 584, the Court of Appeal mentioned this law.

²⁴¹ *An Act to Establish a Legal Framework for Information Technology*, RSQ C-1.1, s. 27

²⁴² *Crookes v. Newton*, 3 SCR 2011, para. 36

²⁴³ In *Weaver v. Corcoran*, 2015 BCSC 165, paras. 267-287. S. 284, the court pronounced as follows: “Until awareness occurs, whether by internal review or specific complaints that are brought to the attention of the *National Post* or its columnists, the *National Post* can be considered to be in a passive instrumental role in the dissemination of the reader postings. It has taken no deliberate action amounting to approval or adoption of the contents of the reader posts. Once the offensive comments were brought to the attention of the defendants, however, if immediate action is not taken to deal with these comments, the defendants would be considered publishers as at that date.”

they contribute to in other circumstances²⁴⁴. In Québec, a Web search service can be held responsible for illegal content it disseminates to the extent that it has knowledge of it. Google's policies, incidentally, offer consumers the possibility of notifying it of such content. They do this either by allowing consumers to send them a court order confirming the illegality of a publication or, in the absence of a court order, provide them with the details of their allegations (Section 2.4.2).

Despite its seemingly simplicity, this process comes up against one major obstacle: if consumers have not obtained a court judgment confirming that a publication is illegal, how can they determine that the content they want removed actually contravenes the law? The company that operates the search engine then faces a dilemma: if it automatically delists the hyperlink, it will be prejudicial to the person who posted the content if it is lawful; if it is not delisted, the consumer who claims to be harmed by its dissemination could, at least in Québec, hold the search engine operator responsible. Pierre Trudel, who has studied the issue in the context of Québec, proposes that in cases when the illegality of a certain content is not obvious, an intermediary should seek independent advice on the situation and base their decision on it²⁴⁵.

However that may be, it is regrettable that clearer rules and procedures for all are not provided for in Canadian law in cases when a content disseminated via a search engine illegally harms an individual. Such rules and procedures would allow conflicting interests to be mediated more effectively and some of the legal unpredictability avoided. Furthermore, as stated in Section 2.5, search engines do not disclose data about the requests they receive concerning allegations about illegal content that are not supported by a judgment, and do not specify what criteria they use to evaluate the cases submitted to them. Greater transparency would be desirable in this regard.

4.2.3. Holding algorithms accountable?

The issue of the responsibility of search engines is often approached in binary fashion: given that a certain reference is accessed by way of its results pages, the search engine is either responsible or it is not. But is that the end of the story? Could the law hold the search engines accountable, not for the references themselves, but rather for the way they are presented?

Since it began its activities, Google has cultivated the idea that the results it generates in response to a keyword search are neutral and objective²⁴⁶. After all, what appears on the screen

²⁴⁴ For example, in *Canadian National Railway Company v. Google Inc.*, 2010 ONSC 3121, a company was able to oblige Google to remove the blog of a third party that it hosted through its Blogspot service because of the defamatory nature of the blog.

²⁴⁵ Pierre Trudel, *La responsabilité sur internet en droit civil québécois*, Rapport préparé pour le colloque de droit civil 2008 de l'institut national de la magistrature, Ottawa, June 13, 2008, pp. 21-22. Online: http://www.pierretrudel.net/files/sites/6/2015/01/TRUDEL_resp_internet.pdf; Nicolas Vermeys, "C-11, la Loi concernant le cadre juridique des technologies de l'information et la responsabilité des intermédiaires techniques québécois : une dualité de régimes (in)utile(s) ?" (2013) 25-3 *Cahiers de propriété intellectuelle* 1051, p. 1066. Vermeys expresses himself as follows on this point: "Is it enough simply to assert the illegality of a content in order to hold the intermediary liable? Should we seek a legal opinion on that? Should the intermediary consult counsel before removing content? These questions remain without a definite answer." [translation]

²⁴⁶ See: <http://www.wired.com/2014/07/google-right-to-be-forgotten-censorship-is-an-unforgettable-fiasco/>

during a keyword search is the automatic product of algorithms applied to an index of sites. The search results, as Google says in its policies, “are a reflection of the content publicly available on the Web²⁴⁷.” Consequently, a search engine could not be held responsible (see Section 2.3).

However, this position fails to mention that the algorithms were programmed by humans. It was human beings who gave them their instructions. The criteria they seek to evaluate, such as the “quality,” “relevance” or “popularity” of a page, are subjective. Behind the algorithms of search engines, there are human decisions to promote certain types of pages rather than others²⁴⁸.

Other human decisions affect the search results. In a wide variety of situations, search engines will modify their indexes one unit at a time. As we saw in Section 2.4, their policies inform us that they can remove search results when they contain certain types of identifiers or sexually explicit images. They can also do so when a publication does not comply with a particular provision of the law. Google says moreover that it can delist pages that in its opinion are “Spam²⁴⁹.” This does not count the many anecdotal cases of discretionary removal for various reasons that the media alleges to have occurred over the years²⁵⁰.

In short, the work of a search engine is based on more subjective criteria and decisions than appears at first glance. Its choices are made by “decision makers” of flesh and blood²⁵¹. With this in mind, it might be useful to question the accountability and transparency of the search engines with regard to their instructions and the results of their algorithms – together with the legal obligations that should accrue to them in this regard.

The issue here is not about delisting the hyperlinks, but the order in which they are ranked. Studies show that the vast majority of Internet users make their choice from among the earliest results they receive in response to a search query; rarely do they consult any of the pages listed after the first page²⁵². In a way, a search engine can be said to be sending a *message* to Web users in its results pages: that the hyperlinks that appear at the top of the first page are the ones that are judged to be the most relevant to their search. To a certain extent, the ranking accorded to the links by the search engines can be thought of as a way of enforcing oblivion, culminating in a form of practical obscurity.

In such a context, is it wrong to propel outdated references about a person to the first few results pages? Are these results really the most relevant ones? From a legal standpoint, should we be able to hold a company responsible for algorithms that unnecessarily dwell on the past? These open questions are difficult to answer without knowing more about the practices of search engine operators. We know, for example, that “the freshness of the content²⁵³” can influence the order of the results in Google: we might think that a post about a person that came out years ago and is no longer relevant to the public, will disappear “naturally” from

²⁴⁷ <https://www.google.ca/intl/fr/policies/fag/>

²⁴⁸ James Grimmelman, “The Google Dilemma” (2009) 53 *New York Law School Law Review* 939, p. 944-945

²⁴⁹ See: <https://www.google.com/insidesearch/howsearchworks/fighting-spam.html>

²⁵⁰ Allyson Haynes Stuart, “Google Search Results: Buried if Not Forgotten” (2014) 15-3 *NCJL & Tech.* 463, p. 476; James Grimmelman, “The Google Dilemma” (2009) 53 *New York Law School Law Review* 939, p. 941-944

²⁵¹ <http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules>

²⁵² See in this regard: <https://chitika.com/google-positioning-value>

²⁵³ <https://www.google.com/insidesearch/howsearchworks/algorithms.html>

among the first results pages, to be replaced by pages that refer to more recent items. But is that really what happens? In the absence of transparency about the exact criteria regulating the algorithms of search engines, it is difficult to ensure that they are based on equitable principles²⁵⁴.

²⁵⁴ For a more thorough discussion of the transparency of algorithms, see: Frank A. Pasquale III, "Restoring Automated Authority to Transparency" (2011) 9-235 *Journal on Telecommunications and High Technology Law* 235

Conclusion: Towards a Canadian solution

At the end of the 19th century, Kodak marketed the first portable cameras. The company sold its devices for a low price, realizing most of its profits on sales of film. This winning business model democratized photography. But the new technology also posed new challenges in terms of privacy. It allowed anyone to invade the privacy of their fellows, without their knowledge. This is what lawyers Warren and Brandeis were concerned about, when in 1890, they published *The Right to Privacy*, a document that was to greatly influence the way the law sees the issue of privacy²⁵⁵.

Just like Kodak long ago, search engines, and Google in particular, have rendered a valuable service to society by democratizing access to knowledge and information. But the possibilities provided by this technology nevertheless blur the distinction between the public and private spheres. Search engines can deliver a snapshot of a person's privacy with an unparalleled degree of efficiency, opening the door to a multitude of indiscretions.

Although the Canadian legal framework offers some solutions to the problems raised by Internet hypermnnesia, gaps still persist. Admittedly, it is possible, in many cases, to ask companies that host personal information to remove it. Similarly, Canadians have recourse against Internet publications that undermine their reputation or their privacy. But sometimes information published legally – against which the person concerned has no recourse – can cause them harm by remaining online forever. A victim of an indictable offense whose name has been published in articles can be dogged by drama for a very long time. Someone who has obtained a pardon for a minor crime can be prevented from rebuilding his life. On a more intimate note, embarrassing or awkward pictures that are not erased from digital memory can have unfortunate repercussions on a person's life.

In practice, even when consumers have rights with respect to content that has been published online, it can be difficult to have them respected. Access to justice is slow and legal proceedings seem poorly adapted to technological realities. Consumers who valiantly do all they can to ensure their personal information is deleted from social media accounts may still see them reappear. While online intermediaries can sometimes be held liable for content they broadcast that illegally infringes a person's rights, the exact obligations of search engines in such cases remain unclear; moreover, little is known about how these issues are managed. In addition, the commercial solutions available to consumers – online reputation repair companies – are costly and there is no guarantee that their attempts to thwart the search engines' algorithms will be successful. This is obviously a luxury that the average consumer cannot afford.

According to several Canadian jurists, however, the right solution is not to adopt a "right to be forgotten" as implemented in Europe²⁵⁶. Legally, implementing such a "right" in Canada, by applying existing Canadian laws on the protection of personal information to Web searches, would raise issues with regard to freedom of expression under the Canadian Constitution.

²⁵⁵ Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy" (1890) 4-5 *Harvard Law Review* 193

²⁵⁶ Pierre Trudel, for example, has published a large number of articles on his blog opposing this right: <http://www.journaldemontreal.com/2014/04/11/la-menace-du-droit-a-loubli>; see also: <http://news.nationalpost.com/full-comment/ann-cavoukian-and-christopher-wolf-sorry-but-theres-no-online-right-to-be-forgotten>

From the consumer's point of view, merely having search engines delist search results as a way of achieving digital oblivion is no panacea. Since unwanted content remains online, only a small amount of computer knowledge would be required to get round these cosmetic measures. For example, an investigator could simply comb through media archives and government databases, (often available online) and restore the person's profile. Since the Internet has no borders, it is not hard to imagine that companies or search engines located in other jurisdictions could quickly provide specialized services to uncover what Google is hiding about certain people.

The greatest fear is that the European approach would threaten the quality of online services offered to consumers, by making the cost of entering the market so high that it would hurt competition. There is no denying that Google is a technology giant that currently dominates the market and that it has been able to handle thousands of requests for delisting received in Europe on a case-by-case basis. But the Internet is forever changing. There is nothing to say that the face of the Web search market will not be altered completely in a few years. Similarly, new, more decentralized ways of organizing the information network could emerge. These new players may not possess the resources to assess, case by case, thousands of individual situations²⁵⁷. Faced with too much responsibility, these small players could simply decide to accede to every removal request they receive, with the result that relevant information about such public figures, professionals or scoundrels would be expunged *en masse* from their search results.

Does this mean that we must reject the European solutions in their entirety? Must we at all costs refuse to increase the number of cases in which consumers can require search engines to delist unfavourable hyperlinks? Not necessarily. Being able to request that search engines delist hyperlinks could be one effective means of protecting consumers against the harmful indiscretions of Web searches. However, considerations of freedom of expression and the need for truly effective solutions militate in favor of a more nuanced approach than one that only targets Web search engines.

As explained in Section 1.3, the "right to be forgotten" is a much broader notion than the right to have unwanted links removed. Implementing such a right would include the removal and depersonalization of content, or in the context of the Web search, making it possible for the authors of pages to tell search engines not to index them. One can also think that the practical obscurity afforded by applying appropriate algorithms to outdated content could provide solutions; the fact that paid services exist that attempt to relegate hyperlinks to lower ranked pages show that this option has relevance. Digital oblivion will also affect the ability of traders or employers to use outdated and irrelevant information on which to base their decisions about a person. Implementing oblivion through solutions provided by technological innovations cannot be ruled out. To ensure adequate protection to consumers, the Canadian reflection on digital oblivion should take all these dimensions into account.

To pursue this reflection further, finding the best solutions to the harm suffered by consumers as a result of digital immortality will require taking into account all the nuances involved in the

²⁵⁷ For example, could the search engine DuckDuckGo, an emerging player in the market that has twenty employees and whose business model is not based on the collection of personal information and appears to be far less lucrative than Google's, be faced with thousands of requests from consumers?

wide range of cases that may arise. There is a difference between a rape victim who is seeking to rebuild her life and a professional who wants to hide his past escapades; between a person who wants to remove the pictures of one drunken night too many from the Web, and one whose past record of public actions cost him employment opportunities. In each case, the severity of the injury, the person who controls the publications, the most effective way of ensuring forgetting, and the legal recourse available can vary greatly.

In our analysis of the policies of search engines, we found that Google already offers opportunities for delisting when people suffer specific harm related to the risk of fraud or identity theft, and more recently, for “revenge porn.” This approach should be expanded in recognition of the fact that some people experience other types of serious harm for which delisting would be a truly effective solution. To illustrate, a particularly disturbing situation of this type that came up during this research is that of crime victims who are named in articles that are published quite legally. This type of article is easily accessible to anyone who does a name search on a popular search engine, but its disclosure can have a crippling impact on the social and personal lives of those named. Similarly, the plight of minors or anyone subjected to humiliating, degrading treatment that has had a significant impact on their social lives also merits consideration.

However, as pointed out by many observers, leaving the role of arbiter largely up to the operators of search engines is a matter for public concern. In Canada, as we have seen, it is the courts that have to juggle the delicate balance between public interest and individual rights (Section 4.1.2). In Europe, the *Google Spain* decision has resulted in search engines operators playing the same role as our courts by having to balancing these factors (Sections 1.4.1 and 2.5.2). Their situation is rendered even more complex by the fact that it involves documents that are often published legally. Technology companies are clearly not courts or legislatures. They are not the ideal forum for determining that some things are too trivial to be forgotten for some people or that things are too terrible to be forgotten for others. Obviously, such decisions must be societal choices. It is up to Canadian society to determine, democratically and transparently, how far its digital clemency extends.

In order for society to make informed choices, it must have access to all the necessary information. There was one thread that ran throughout this research: the issue of transparency. However laudable, the search engines’ commitment to the transparency of their operations is incomplete. They do not provide data on every type of removal request they receive, on the alleged motives of those who make these requests or on the answers they give to them. Similarly, they provide only a very general account of the criteria governing instructions for search algorithms, which may yet be judged to play a deciding role in the process of procuring digital oblivion. Access to this information seems essential if Canadian society is to understand the difficulties faced by consumers, to identify the problems that need to be redressed and to develop clear rules and procedures for all.

Finally, we perhaps have to accept that, sooner or later, society will change. Kodak, in democratizing photography, changed people’s relationship to images of themselves, for better or for worse. In the digital age, new social codes are sure to emerge that will set new limits on what we see and how we behave online. At a time when online anonymity allows anyone to besmirch someone else’s reputation, by either maliciously posting incriminating content about

them, or causing them harm in some other way, it has to be acknowledged that individuals share part of the responsibility. Learning how to use the Internet ethically and being able to relativize what one finds there – and understanding that the past is the past – are a necessary part of the equation.

In light of the foregoing, we issue the following recommendations:

Recommendations to the federal and provincial governments:

- **Option consommateurs recommends that innovative, simple and effective mechanisms be developed to allow consumers to assert their rights when content posted online infringes their privacy or reputation.**
- **Option consommateurs recommends that the obligations of online intermediaries, when they receive notice that they are allegedly disseminating illegal content, be clarified.**
- **Option consommateurs recommends that the technology companies that host data created or generated by consumers offer them simple and effective suppression mechanisms and do not store this data when consumers request that it be deleted.**
- **Option consommateurs recommends that the difficulties posed by Web hypermnnesia be recognized and that research be undertaken on comprehensive solutions to effectively limit the damage it can do. In their reflections on this recommendation, governments should consider:**
 - **the acute need for greater transparency about the practices of search engines and the criteria that regulate their algorithms;**
 - **the wide variety of harmful situations that can result from the hypermnnesia of the Web and the best way to respond to each situation in the digital environment;**
 - **the possibility of increasing the responsibility of search engines when removing hyperlinks offers an effective solution to an injurious situation – and the need for clear rules in this regard;**
 - **the role of the organizations and individuals who make decisions on consumers based on their virtual profile.**
- **Option consommateurs recommends supporting educational activities on online ethics and on the protection of privacy on the Internet.**

Recommendations to the search engines:

- **Option consommateurs recommends that search engines be more transparent about delisting practices and the criteria used to regulate search algorithms.**
- **Option consommateurs recommends ensuring that the time elapsed since the publication of a page be one of the criteria in determining its relevance when a user searches for a person.**
- **Option consommateurs recommends that the types of cases in the policies that qualify for removal be increased to cover other types of harm.**

Recommendation to consumers:

- **Consumers should inform themselves of the means available for removing and protecting their digital data and the best practices for protecting their online reputation.**