THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

CCCA
ACCJE
Canadian Corporate Counsel Association
Association canadienne des conseillers (ères) juridiques d'entreprises

May 1, 2018

Via email: OPC-CPVPconsult2@priv.gc.ca

Daniel Therrien
Privacy Commissioner of Canada
Office of the Privacy Commissioner of Canada
30 Victoria Street – 1st Floor
Gatineau, QC K1A 1H3

Dear Commissioner Therrien:

Re: Draft Position Paper on Online Reputation

The Canadian Bar Association Privacy and Access Law Section, the Children's Law Committee and the Canadian Corporate Counsel Association (the CBA Sections) are pleased to comment on the Draft Position Paper on Online Reputation (the Position Paper) released by the Office of the Privacy Commissioner of Canada (OPC) in January 2018.

The CBA is a national association of 36,000 members, including lawyers, notaries, law students and law professors across Canada, with a mandate to seek improvements in the law and the administration of justice. The CBA Privacy and Access Law Section comprises lawyers with an in-depth knowledge of privacy and access to information law, the CCCA comprises in-house counsel working for public and private companies, not-for-profit associations, government and regulatory boards, hospitals and municipalities, and the Children's Law Committee comprises lawyers with expertise in children's law issues who advise on matters affecting Canadian children.

The CBA Sections have made numerous submissions on the interpretation of *Personal Information Protection and Electronic Documents Act* (PIPEDA) since its enactment. Recently, the CBA Sections commented on the OPC's Draft Guidelines for Obtaining Meaningful Online Consent[1] and responded to the House of Commons Committee on Access to Information, Privacy and Ethics' (the ETHI Committee) study of PIPEDA.

[1] Canadian Bar Association, *PIPEDA: Draft Guidelines for Obtaining Meaningful Online Consent* (Ottawa: December 2017), available online; *PIPEDA* (Ottawa: March 2017), available online.

General Comments

The CBA Sections support the OPC's efforts to seek feedback from stakeholders on its position papers and guidance documents. We agree with the OPC that existing privacy laws, designed in an era when these issues did not exist should be studied further by Parliament. Privacy legislation, as well as the *Canadian Charter of Rights and Freedom,*[2] are interpreted today in a different context than when they were originally drafted. As the internet broadly, and search engines specifically, are significant sources of information for Canadians, online reputation and disclosure of personal information online are important issues for regulators, policy makers and legislatures to examine. While the CBA Sections do not take a position on matters of policy best left to Parliament, we offer our comments on the legal analysis and implications of the OPC's Position Paper and the right to de-index or right to be forgotten in the Canadian legal landscape.

Application of PIPEDA to search engines

"Collection, use and disclosure" of personal information

In its Position Paper, the OPC concludes that search engines fall under the scope of PIPEDA because they are engaged in the "collection, use or disclosure" of personal information. Members of the CBA Sections have differing views on this analysis.

Some members support the OPC position that search engines, by indexing webpages containing personal information, and returning links to those pages in search results, are "collecting, using and disclosing" personal information within the meaning of PIPEDA. These members agree with the OPC that search engines are not passive intermediaries, and that the inextricable link between advertising and provision of search services leads to the conclusion that search engines are engaged in commercial activity.

Other members of the CBA Sections argue that search engines perform something akin to a journalistic function and therefore fall outside the ambit of PIPEDA. Others look to the Supreme Court of Canada defamation case, *Crookes v. Newton,*[3] which determined that hyperlinks are not publications, but references taking the user to other sources. Extrapolating this analysis to PIPEDA, they conclude that indexing web content is not collection or use of personal information as it is understood under PIPEDA, but rather, search engines facilitating the location of web content created by others.

Commercial activity

There are also differing opinions among the CBA Sections whether search engines are engaged in commercial activity. While recognizing that some aspects of search engine indexing are commercial in nature, such as paid advertising, some members argue that much of the indexing that does occur does so outside of a commercial relationship:

> search results are typically provided at no cost to the user nor the sites being indexed. Indeed, all the activity behind search – indexing content, developing algorithms to identify relevant results, and the display of those results – fall outside a conventional commercial transaction. There may be paid results or

---

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

3 2011 SCC 47.

other advertising displayed with some search results, but those are arguably secondary to the indexing, ranking, and display of the relevant links.[4]

PIPEDA's consent requirement

Even if search engines are subject to PIPEDA, the CBA Sections question how PIPEDA could practically be applied. Consent has long been posited as the fundamental underpinning of PIPEDA; and assuming search engines fall within the scope of the legislation, they would be required to obtain consent before including individuals in any search results. This would be an untenable requirement that could lead to overwhelming non-compliance. The OPC acknowledged this in its Position Paper, stating "it may not be practicable for an intermediary such as a search engine to obtain consent to index all webpages on the Internet that contain personal information," and proposed creating an exception. Some members of the CBA Sections argue that this begs the question: if search engines would be exempt from a fundamental underpinning of PIPEDA anyway, are they intended to fall under its ambit? These issues warrant further clarification.

De-indexing and source takedown obligations in PIPEDA

The OPC Position Paper determined that the application of PIPEDA gives rise to certain de-indexing and source takedown obligations on the part of search engines. Again, members of the CBA Sections have differing views on this analysis.

Some members of the CBA Sections view this as a sound and reasoned interpretation of PIPEDA. They look to Principle 4.6 and section 5(3) of PIPEDA as creating the search engines' de-indexing obligations. Principle 4.6 (the accuracy principle) articulates the obligation of businesses to ensure that personal information is accurate, complete and up-to-date, taking into account individual interests. This principle arguably includes an individual's right to have search results amended, if the individual is successful in challenging the accuracy, completeness or currency of the results generated by a search. Section 5(3) of PIPEDA – which qualifies an organization's right to collect, use and disclose personal information: "only for purposes that a reasonable person would consider are appropriate in the circumstances" – establishes further limitations on displaying search engine results. In circumstances where a reasonable person would not consider it appropriate that content containing their personal information was identified by a search engine as "relevant," for example, where the content is unlawful, or where the information may cause significant harm to the individual, a search engine, once notified of one of these circumstances, should de-index the inappropriate web content.

These members also look to Principles 4.3.8 and 4.5.3 of PIPEDA as imposing obligations on search engines for source takedown in certain instances. Pursuant to Principle 4.3.8, individuals have the right to withdraw consent subject to legal or contractual restrictions. Further, Principle 4.5.3 requires that personal information that is no longer needed be destroyed, erased or made anonymous. These principles, when applied together, mean that individuals should have a right to have information they provided to a website removed. Where personal information is shared by someone other than the person to whom it relates (such as where information is re-posted), if the person who originally posted the information has not given their consent, they should have a right to have the information removed. Furthermore, the accuracy principle and the appropriate purposes section should apply to require the website to remove inaccurate or inappropriate information.

---

4 Michael Geist, Special to the Globe and Mail, "Why a Canadian right to be forgotten creates more problems than it solves" (January 26, 2018), available online.

Other members of the CBA Sections question whether de-indexing and source takedown obligations exist under PIPEDA. They believe that the right to be forgotten is not addressed directly in PIPEDA and the OPC's interpretation that PIPEDA requires removal of links from search indexes or lowering of rankings to obscure search results extends well beyond an organization's obligation under PIPEDA to update and correct inaccurate information.

They also take issue with the OPC's arguably more far-reaching recommendation that search engines be empowered to block Canadians from accessing the links in question by using geo-fencing technologies:

> Mandated use of blocking technologies as well as a parallel recommendation for a notice-and-takedown system for content that is not found under current Canadian law represents a dramatic departure from the existing Internet rules of the road. These forms of regulation cannot simply be read into PIPEDA by the Privacy Commissioner, but rather should require careful review and legislative reforms by Parliament."[5]

Further, they argue that applying PIPEDA's statutory withdrawal right (principle 4.3.8) to search engines suggests that individuals have a general right to prevent search engines from indexing any personal information about them, for almost any reason. This would have troubling implications.

The recent Irish High Court decision in *Savage v Data Protection Commissioner* illustrates this issue: Mark Savage, a politician and candidate in local elections, ran on a family values platform and requested that Google remove a link to a Reddit post that portrayed him as homophobic. Google refused to de-index the post. The Irish Circuit Court focused on the description of Savage in the URL and page title as it appeared on Google's search results. However, the High Court concluded that there was a duty to look at the underlying article. In looking at the article, the Court held that it was not inaccurate data as it was an opinion validly expressed by a Reddit user. The decision looked to the interpretation of "accurate" in Ireland's Data Protection Acts 1998 & 2003. Savage, ultimately, was relying on the right to be forgotten to remove content that did not work in his favour.

Appropriate role of internet intermediaries

The conclusions drawn by the OPC that search engines might be asked to lower the rank of a search result, flag the result as inaccurate or incomplete, or determine relevance or harm (weighed against the public interest), would vest search engines with significant editorial power. Some members of the CBA Sections have concerns about the appropriate role and capacity of search engines, and other Internet intermediaries, to act as content moderators.

These members believe it is unreasonable and inappropriate to posit search engines in a quasi-judicial role regulating privacy rights. Determinations of reputational harm are complex, challenging and highly contextual. Deciding what is in the public interest is difficult for a court, let alone a search engine. For example, would a negative review on *ratemyprofessor* or *ratemyMD* be considered in the public interest? The Court's commentary in *Grant v Torstar Corp*[6] is instructive: "the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached." While doctors and professors are not public figures, they are professionals and arguably their work affects the welfare of citizens. Search engines and other internet intermediaries do not have the level of familiarity with privacy, in all of its dimensions, in order to be vested with this level of privacy regulation.

---

5 *Supra* note 4.

6 2009 SCC 61.

The OPC argues that search engines already perform these functions, for example by removing content that violates terms of service. The reality is that very little is known about the decision-making processes of search engines. Moreover, their application of internal controls is very different from making privacy law determinations under the *Charter*.

While expedient remedies for issues with online reputation are valuable, any requirement on the part of search engines to de-index should come with responsible measures in place to address questions such as how search engines ought to engage with their analysis, whether source authors should be notified of the request for de-indexing, and if there are opportunities to dispute a request for de-indexing. Decisions made without the necessary expertise and appropriate balancing of competing priorities increase the chances of inconsistent approaches to privacy interpretation.

Should there be a right to be forgotten in Canada?

The CBA Sections do not take a specific stance on whether there should be a right to be forgotten in the Canadian legal landscape, however, we believe it is an important question that merits attention, and we discuss some considerations to take into account.

A need for better reputational privacy protection

Some members of the CBA Sections are of the view that the existing legal framework for protecting personal reputation has not kept up with technology, and Parliament needs to step in to determine the appropriate balance between the right of Canadians to control data about themselves and the easy availability of sensitive personal data in the online context. As the Court stated in *Hill v. Church of Scientology of Toronto*:

> Although it is not specifically mentioned in the *Charter,* the good reputation of the individual represents and reflects the innate dignity of the individual, a concept which underlies all *Charter* rights. It follows that protection of the good reputation of an individual is of fundamental importance to our democratic society. [7]

Before the challenges presented by new technologies and online businesses (including search engine services, social media websites and other web hosting services), individuals could, for the most part, control the dissemination of their personal data. Data protection was not a major issue. Defamation law was the primary legal tool for controlling one's reputation. That has changed, and radically so. Individuals need to be concerned not only about defamatory comments, but also about information that (while perhaps not defamatory) is dated, de-contextualized or unfair while at the same time persistent, easily available to anyone and readily distributed to others. As the OPC states,

> in the digital environment, judgments are generally formed on information people read about others, or images they see, often without the benefit of personal contact and not necessarily in the same context in which it was intended. Moreover, information, once posted online, gains characteristics that affect reputation – it can easily be distorted, is persistent and can be extremely difficult to remove.[8]

Despite the Court's efforts to uphold individual privacy protection,[9] some members believe individual privacy has suffered and Canadian laws need to be re-examined to appropriately balance privacy and free expression in the online context in a manner that reflects Canadian societal values.

---

7 1995 2 SCR 1130 at para 120.

8 Draft OPC Position on Online Reputation, Executive Summary.

9 For example, the Court's definition of "reasonable expectation of privacy" as a normative rather than merely descriptive concept: *R. v. Tessling*,

Arguably, the balance between privacy and free expression established by lawmakers needs to be re-examined in light of new technologies and business models based on collection and exposure of personal information without content curation or liability. The growing treatment of online businesses' proprietary services (e.g., search, social media, web hosting) as important vehicles of free expression (with little legal responsibility for publishing illegal or socially undesirable content) has concerning implications for privacy protection.

Existing forms of recourse

Other members of the CBA Sections argue that the existing means by which an individual can manage use of their information online weighs against introducing a right to be forgotten in Canada. Information shared by third parties may be subject to recourse under a number of existing laws, including defamation, copyright infringement, cyber-bullying or criminal laws. A substantial body of case law on defamation would apply to information online that is incorrect and misleading or harms someone's reputation. Editorial corrections in news sources also pose an option for recourse. Further, information in source documents indexed by search engines may be subject to PIPEDA or other privacy laws across Canada. These forms of recourse properly frame the issue as between the affected individual and the person who created or has control of the content, rather than placing content mediation power in the hands of search engines.

Concealed Censorship and Unequal Access to Data

Some members of the CBA Sections also note that a right to be forgotten is not a panacea for issues of reputational harm and has its own challenges. It is often criticized as being a "concealed form of censorship".[10] Since companies could incur liability for not removing results objected to, there may be an inclination to err on the side of caution and remove more than necessary, leading to private censorship. This must be weighed against the importance of accessible and publically available information.

A right to be forgotten could result in a two-tiered system of publicly available information. Google recently argued that de-indexing was ineffective and unfair: "Many have likened the European court's ruling to removing the cards from a library card catalog but leaving the books on the shelf. … Decisions to delist URLs can affect users' access to media properties, past decisions by public figures and information about many other topics."[11] Online search engines provide access to an incredible wealth of information for free, and the right to be forgotten could create unequal access to data, where information is available only to those with the means or resources to obtain it.

Criteria and Enforcement

If Parliament were to introduce a right to be forgotten, it should take note of the *Crouch v Snell*[12] case, which struck down Nova Scotia's *Cyber-safety Act.*[13] In this case, the *Cyber-safety Act* failed the *Oakes*[14] test on the basis that it did "not provide sufficiently clear standards to avoid arbitrary and

---

10 Gratton, Eloise and Polonetsky, Jules, "Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada" (April 2016), available online.

11 Google Canada, "Can the right to be forgotten find application in the Canadian context and, if so, how?". Submissions received for the consultation on online reputation, Office of the Privacy Commissioner of Canada (August 2016), available online.

12 2015 NSSC 340.

13 S.N.S. 2013, c. 2.

14 *R. v Oakes*, [1986] 1 S.C.R. 103,

discriminatory applications."[15] To avoid these issues, Parliament would be well advised to adopt clear and precise criteria for any de-indexing or removal of content.

As well, the recent decision in *R. v. Canadian Broadcasting Corporation*[16], which dealt with a publication ban under the *Criminal Code*, is worthy of note. This case illustrates the challenges, specifically, of enforcing statutory publication bans online, and more broadly, protecting rights of removal of online information without corresponding enforcement capabilities.

Charter Context

Parliament must also consider the context in which a right to be forgotten may operate in Canada. Canada's privacy laws are framed and operate differently than those in Europe, where the right has emerged[17]. In Europe, privacy and freedom of expression are recognized to have equal weight. In Canada, although statutory privacy rights have been found to be quasi-constitutional, privacy is not an inviolable right – it is a right read into section 7 of the *Charter* that must be balanced against competing priorities, including the right to freedom of expression[18]. The right to freedom of expression is constitutionally enshrined in the *Charter* and represents a critical piece of our democratic fabric. As the Court stated: "freedom of expression and respect for vigorous debate on matters of public interest have long been seen as fundamental to Canadian democracy."[19] *Grant v Torstar Corp*. is informative: although looking at privacy rights in the context of the common law of defamation, the Court found that privacy protection/protection of reputation should not go as far as to have a chilling effect on freedom of expression. There is a clear tension between introducing a right to be forgotten in Canada and complying with the constitutional status of freedom of expression. Any de-indexing or source takedown obligations will need to be weighed against the right to freedom of expression and access to publicly available information.

Other Tools for Privacy Protection

The CBA Sections have long supported the continued use of a multifaceted "toolkit" approach to privacy protection in Canada, and we encourage the OPC to consider other options found in the PIPEDA toolbox to address some concerns that the European "right to be forgotten"[20] seeks to address, particularly for accuracy and appropriate purposes. As stated in the ETHI Committee's February 2018 report,[21] PIPEDA does not operate in a vacuum, and existing provincial and federal laws also come into play with respect to reputation and privacy.

While the OPC Position Paper outlines remedies from search engines to address issues with reputational harm, it does not mention remedies from organizations using the personal information that surfaces in search results. These organizations have clear and direct obligations related to both purpose and accuracy.

---

15 *Ibid*. at para 138.

16 2018 SCC 5.

17 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April on the protection of individuals with regard to processing of personal data and on the free movement of such data (General Data Protection Regulation), Art. 17, available online.

18 *Supra* note 1.

19 *Supra* note 8 at para. 42.

20 *Supra* note 17.

21 House of Commons Standing Committee on Access to Information, Privacy and Ethics, "Towards Privacy By Design: Review of the *Personal Information Protection and Electronic Documents Act*", (February 2018), available online.

When it comes to permitted purposes, PIPEDA is clear that an organization may only collect and use personal information for purposes that a reasonable person would consider appropriate in the circumstances. Although organizations do not have an obligation to constantly update personal information (as doing so could have the unintended consequence of resulting in over collection or introduce an error in the information) they do have an obligation to ensure the personal information they intend to use is as "accurate, complete and up-to-date as is necessary for the purpose". The use of outdated personal information or information out of context may not only be considered inappropriate in the circumstances, but might also conflict with the organization's accuracy obligations. Organizations must take into account the interests of the individual and take steps to minimize the possibility that inappropriate information (such as outdated personal information or information taken out of context) may be used to make a decision about the individual.

As part of ongoing outreach efforts, the CBA Sections encourage educating organizations about their use of online information to ensure the purpose is appropriate in the circumstances and the information is as accurate as is necessary for that purpose.

The special case for children and youth

The advent of social media and new technologies poses particular risks to the online reputation of children and youth. Recent Parliamentary studies,[22] special reports by independent commissions,[23] and a flurry of legislative reform responding to cyber-bullying[24] in response to the deaths of young Canadians Amanda Todd and Rehtaeh Parsons illustrate the social challenges surrounding the use or misuse of technologies by children and youth.

The CBA Sections support the emphasis in the OPC's Position Paper on the special case for children and youth. We encourage Parliament to afford Canadian children expansive privacy protection in accordance with their constitutional rights. The Court has recognized the importance of protecting the privacy rights of young Canadians and underlined that, consistent with the privacy rights in the *United Nations Convention on the Rights of the Child* (UNCRC), "recognition of the inherent vulnerability of children has consistent and deep roots in Canadian law."[25]

The UNCRC, of which Canada is a party, proclaims the right of all children to privacy. Parties to the UNCRC are expected to "[e]ncourage the development of appropriate guidelines for the protection of the child from information and material injurious to his or her well-being." Article 16 speaks to the child's right to protection against "unlawful attacks upon his or her honour and reputation", and Article 17 outlines the child's right to access information and the role of mass media in ensuring that children have access to information that is "aimed at the promotion of his or her social, spiritual and moral well-being and physical and mental health." The best interests principle (Article

---

22 Senate of Canada, *Cyberbullying Hurts: Respect for Rights in the Digital Age,* (December 2012), available online

23 MacKay, Wayne, *Respectful and Responsible Relationships: There's No App for that* Report of the Nova Scotia Task Force on Bullying and CyberBullying(Nova Scotia: February2012), available online; *There Ought to Be a Law: Protecting Children's Online Privacy in the 21st Century*: Discussion Paper of the Working Group of Canadian Privacy Commissioners and Child and Youth Advocates (Ottawa: November 2009), available online.

24 *Reporting Bullying Regulation* Manitoba Public Schools Act, Man Reg 37/2012; *Promotion of Respectful and Responsible Relationships Act*, Statutes of Nova Scotia, SNS, 2012 C. 14; *An Act respecting Private Education*, RSQ, c. E-9.1, June 15, 2012; *An Act to Amend the Education Act*, SNB, 2012; *Ontario Education Act*, RSO 1990, c.E.2.

25 *Ibid*.

3) and the child's right to life, survival and development (Article 6) are also important. The UNCRC illustrates the importance of governments sedulously protecting the privacy rights of children and youth. Governments must have regard for the developmental stages of children and youth and the risks to which they may expose themselves via their online activities.

Canadian criminal law also protects young people from stigma that might affect their futures, even in the context of criminal behaviour. The strict privacy protections in the *Youth Criminal Justice Act*[26] are a proportional limit on freedom of expression,[27] and the reduced moral blameworthiness of young people has been recognized as a principle of fundamental justice.[28] These laws also speak to the appropriateness of having mechanisms in place to protect children and youth's online reputation. If Parliament were to introduce a right to be forgotten, it could pursue a graduated approach that prioritizes legal protections for children and youth. Parliament should also look to the protections of minors in Europe[29] and the United States[30] and ensure that Canadian children are afforded the same protections.

Conclusion

The CBA Sections appreciate the opportunity to comment on the Position Paper. Online reputation is an important issue that requires careful study. Parliament must be mindful, however, that PIPEDA and other private sector privacy legislation cannot be the catch-all for issues that arise from the ongoing evolution of technology. Even the OPC, while arguing in its Position Paper for a right to be forgotten/right to de-index under PIPEDA, has asked Parliament to carefully study the issue and review the proposed balance to be struck. The uniqueness of the Canadian *Charter* context and the far-reaching implications for freedom of expression and access to publicly available information, underscores the need for legislative and policy guidance in this unchartered area.

We trust that our comments are helpful and would be pleased to offer any further clarification.

Yours truly,

(original letter signed by Gilian Carter for Suzanne Morin, Nick Slonosky and Cheryl Milne)

Suzanne Morin
Chair, CBA Privacy and Access Law Section

Nick Slonosky
Canadian Corporate Counsel Association

Cheryl Milne
Chair, Children's Law Committee

---

26 *F.N. (Re)*, [2000] 1 S.C.R. 880 [this case considered the previous *Young Offenders Act*, but the principles apply equally to the *Youth Criminal Justice Act*]; see also *R. v. L.T.C.*, 2009 NLCA 55 (CanLII), leave to appeal to SCC refused (2010), 297 Nfld & PEIR 131*n* where early destruction of youth records held to facilitate rehabilitation and reintegration of the young person into society.

27 *Re Southam Inc. and The Queen (No. 1)*, 41 O.R. (2d) 113; 146 D.L.R. (3d) 408.

28 *R. v. D.B.*, [2008] 2 SCR 3.

29 European states have stringent compliance directives in place regarding the right of erasure and the right to be forgotten: see *supra* note 17, and Court of Justice of the European Union, *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González* (2014), Case C-131/12, available online.

30 California has recently legislated the protection of minors: *Privacy Rights for California Minors in the Digital World*, available online.