



Office of the  
Privacy Commissioner  
of Canada

Commissariat  
à la protection de  
la vie privée du Canada

[Home](#) → [About the OPC](#) → [What we do](#) → [Consultations](#) → [Completed consultations](#)  
→ [Consultation on online reputation](#)

# Draft OPC Position on Online Reputation

---

## Table of Contents

[\*\*Executive Summary\*\*](#)

[\*\*Introduction\*\*](#)

[\*\*Objective\*\*](#)

[\*\*A. De-Indexing\*\*](#)

[\*\*B. Source Amendment/Takedown\*\*](#)

[\*\*C. The special case of youth\*\*](#)

[\*\*D. Improving Sites' Practices\*\*](#)

[\*\*E. Improving Education\*\*](#)

[\*\*F. Promoting further research\*\*](#)

[\*\*G. Legislative solutions\*\*](#)

[\*\*Conclusion and next steps\*\*](#)

### **!** Notice

---

This draft policy position has been published for discussion and commenting purposes as part of our work on the issue of [Reputation and Privacy](#) (</en/about-the-opc/opc-strategic-privacy-priorities/the-strategic-privacy-priorities/>). Please see our [Consultation on online reputation](#) (</en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/>) web page for more information.

## Executive Summary

When the Office of the Privacy Commissioner of Canada (OPC) named “Reputation and Privacy” as one of its [strategic privacy priorities for 2015-2020](#) (</en/about-the-opc/opc-strategic-privacy-priorities/>), we set as our goal that:

*[We] will have helped to create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.*

To advance this goal, we undertook a [consultation and call for essays](#) (/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/) on the issue of online reputation. Based on the 28 submissions received, along with our own analysis, the OPC has published a draft Position on Online Reputation that champions solutions that balance freedom of expression and the privacy interests of individuals.

We have heard from stakeholders and the Canadian public that while they recognize the personal and professional benefits of participating in the online world, they are increasingly concerned about their online reputation. In focus groups, Canadians told us they are concerned that they lack control to protect themselves from risks related to online reputation. Several stakeholders also raised the importance of respecting freedom of expression.

The development of reputations online is complicated because, 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.

## Solutions

It is clear that Canadians need better tools to help them to protect their online reputation.

The OPC's draft position highlights existing protections in Canada's federal private sector privacy law, identifies potential legislative changes and proposes other solutions for consideration.

These measures include the right to ask search engines to de-index web pages that contain inaccurate, incomplete or outdated information; removal or amendment of information at the source; and education to help develop responsible, informed online citizens.

## De-Indexing and Source Takedown

Two key mechanisms identified for enhancing one's control over their online reputation – both of which can be found within PIPEDA – are *de-indexing* and *source takedown*.

De-indexing is the process by which a webpage, image or other online resource is removed from search engine results when an individual's name is entered as the search term. Source takedown refers to the removal of the content from the internet.

With respect to de-indexing, the OPC is of the view that PIPEDA applies to a search engine's indexing of online content and display of search results. As such, search engines must meet their obligations under the Act.

This includes allowing individuals to challenge the accuracy, completeness and currency (the extent to which the information is up-to-date) of results returned for searches on their name. Such challenges should be evaluated on a case-by-case basis, and decisions to remove links should take into account the right to freedom of expression and the public's interest in the information remaining accessible. Additional detail, criteria and discussion about this mechanism are presented in the report.

If an individual is able to successfully challenge the search result based on the above, it should be de-indexed. However, lowering the ranking of a result or flagging a link or content as inaccurate or incomplete could be sufficient alternatives in some cases.

With respect to source takedown, PIPEDA provides individuals the right to withdraw consent, and requires that personal information that is no longer needed be destroyed, erased or made anonymous. Taken together, this implies that individuals should have the ability to remove information that they have posted online.

Where the personal information in question has been posted by others, individuals do not have an unqualified right to remove it. However, similar to de-indexing, individuals should be provided a mechanism by which they can challenge the accuracy, completeness and currency of the information and, where such a challenge is successful, to have the information corrected, deleted or augmented, as appropriate.

In either of the above cases, where matters cannot be resolved with a website or search engine, individuals may lodge a formal complaint with the OPC.

While, in combination, the abilities to request de-indexing and/or source takedown of information in certain circumstances are similar to the “Right to Erasure (Right to be Forgotten)” in the EU’s General Data Protection Regulation (GDPR), this paper does not import a European framework into Canada. Rather, it is an interpretation of current Canadian law, and the remedies related to online reputation that can be found therein.

While it is important to take action on de-indexing – as reputation is currently at risk, and the solutions we’ve proposed are, in our view, both balanced and workable – the report also recommends Parliament undertake a study of this issue. Elected officials should confirm the right balance between privacy and freedom of expression in our democratic society.

## Education

The report also emphasizes the importance of privacy education.

It is why OPC – along with its provincial and territorial counterparts – have sent a [joint letter](/en/opc-news/news-and-announcements/2017/let_171103/) (/en/opc-news/news-and-announcements/2017/let\_171103/) to the Canadian Council of Ministers of Education calling for privacy protection to be incorporated into curriculum for digital education.

A rights-based privacy education program will serve to develop good online citizens who have both the technical knowledge needed to protect themselves as well as a strong sense of how and why it is important to act responsibly online.

Not only is it important to educate young people, indeed all Canadians, on the use of mechanisms to control reputation such as takedown procedures, privacy settings and emerging privacy enhancing technologies, it is equally important to emphasize the importance of thinking about the potential impacts of one’s actions on others.

The OPC, in cooperation with other stakeholders, will continue to create resources to help inform people of reputational risks and privacy protections.

## Other proposals

Beyond de-indexing, source takedown and education, the report sets out a number of mechanisms and proposals aimed at improving individuals’ control of their online reputation:

- That Parliament consider enshrining in law the near absolute right for youth to remove any content from the internet that they have posted themselves or information they have provided to an organization to post;
- That Parliament consider providing youth with some ability, upon reaching the age of majority, to request and obtain removal of online information posted about them by their parents or guardians;
- That the OPC proactively address systemic or sector-wide problems related to online reputation, for instance, where vulnerable groups are concerned;
- That the OPC encourage research, development and adoption of new solutions for protecting online information, in part through its Contributions Program; and
- That an industry-wide code of practice be developed for takedown policies, privacy defaults and procedures.

## Next steps

After seeking stakeholder views on the proposals outlined in this draft position paper, the OPC will finalize its position and develop an action plan to put the new measures into practice. We invite you to review our complete Position on Online Reputation in the following pages.

## Introduction

In January 2016, the Office of the Privacy Commissioner of Canada (OPC) launched a consultation and call for essays on the issue of online reputation, guided by a [discussion paper](/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or_201601/) (/en/opc-actions-and-decisions/research/explore-privacy-research/2016/or\_201601/).

Through this consultation, the [OPC \(Office of the Privacy Commissioner of Canada\)](#) solicited input about new and innovative ways to protect reputational privacy, one of the [OPC \(Office of the Privacy Commissioner of Canada\)](#)'s strategic privacy priorities. The aim was to enrich the public debate, ensure that we are in a better position to inform Parliament of a variety of solutions for addressing issues related to online reputation, and develop a policy position on this issue.

We received [28 submissions from a variety of stakeholders](#)

(/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub\_or\_04/)

. We have taken this feedback, in combination with our own analysis and experience, and used it to develop our position and recommendations with respect to privacy and online reputation. This includes our views on what protections currently exist under Canada's federal private sector privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA), what legislative changes (to [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) or to Canadian law more generally) might or should be considered to improve upon the *status quo*, and what other solutions should be promoted in relation to this matter.

## Objective

When the [OPC \(Office of the Privacy Commissioner of Canada\)](#) named "Reputation and Privacy" as one of its [strategic privacy priorities for 2015-2020](#) (/en/about-the-opc/opc-strategic-privacy-priorities/), we set as our goal that:

*[We] will have helped to create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment.*

Our consultation process has, if anything, validated the importance of this goal. Many submitters highlighted the legitimacy of providing individuals with at least some level of control over their online reputation. Where views varied – and where this paper will focus – was in defining the extent to which individuals should be permitted to control their online reputation in light of other important interests under existing law, and the mechanisms by which they could do so.

## *Freedom of Expression Considerations and the Balance with Privacy Interests*

Of particular interest to submitters, and to our office, in the evaluation of reputation control mechanisms was the interplay between the protection of privacy and other societal values such as freedom of expression. For instance, while privacy interests may point in favour of allowing individuals to control the presence or accessibility of personal

information, there will be in some cases a countervailing interest in ensuring that that information remains widely available. It is therefore necessary – and a primary objective of this paper – to consider how to strike an appropriate balance between an individual’s privacy interests and that of other relevant values, including freedom of expression.

As a general matter, the right to freedom of expression protected by section 2(b) of the *Canadian Charter of Rights and Freedoms* is broad in scope and covers any activity that “conveys or attempts to convey meaning” with the exception of violence. <sup>1</sup> (#fn1) The Supreme Court of Canada has consistently held that the concept of freedom of expression is to be given a “large and liberal interpretation,” <sup>2</sup> (#fn2) and has found that freedom of expression protects not just speakers but listeners as well, and, in particular, the right of individuals to receive and access information that is of public interest. <sup>3</sup> (#fn3)

The Supreme Court has also noted that while freedom of expression is broad, it is not absolute. <sup>4</sup> (#fn4) The challenge therefore is to consider measures that appropriately balance an individual’s privacy and reputational interests with the equally important values protected by freedom of expression. <sup>5</sup> (#fn5)

Three values have been identified by the Supreme Court which underpin the right to freedom of expression: individual self-fulfillment, the search for truth and the promotion of democratic discourse. It is worth noting that the protection of reputation can advance these same interests; for instance, individuals with unduly damaged reputations may not be able to fully participate in public discourse – they may be ignored, not believed, or have their contribution to the “marketplace of ideas” judged based on their reputation instead of the content.

In *Hill v. Scientology* <sup>6</sup> (#fn6), the Supreme Court stated:

[T]o most people, their good reputation is to be cherished above all. A good reputation is closely related to the innate worthiness and dignity of the individual. It is an attribute that must, just as much as freedom of expression, be protected by society’s laws.

Democracy has always recognized and cherished the fundamental importance of an individual. That importance must, in turn, be based upon the good repute of a person. It is that good repute which enhances an individual’s sense of worth and value. ... A democratic society, therefore, has an interest in ensuring that its members can enjoy and protect their good reputation so long as it is merited.

Similarly, in *Grant v. Torstar* <sup>7</sup> (#fn7), the Court wrote:

[T]he plaintiff’s interest in reputation may be just as worthy of protection as the defendant’s interest in self-realization through unfettered expression. ... Charter principles do not provide a licence to damage another person’s reputation simply to fulfill one’s atavistic desire to express oneself.

While the above statements are both found in judgments related to libel, the argument can be extended to measures that protect reputation more generally – including privacy law.

Given the above, we have sought to avoid (to paraphrase a [submission](/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_09/)) “fetishizing” either an individual’s ‘right’ to curate their reputation or other values such as freedom of expression. Rather, we have endeavoured to develop a position which respects both freedom of expression and privacy interests.

In our view, this balance can best be achieved in the context of online reputation by considering whether the accessibility of personal information is in the public interest. In general, where there is a sufficient public interest in the information remaining accessible, this will normally trump an individual’s desire to control access to their personal

information that has been lawfully published online. The Supreme Court of Canada has offered the following definition of “public interest” in the context of defamation law:

To be of public interest, the subject matter “must be shown to be one inviting public attention, or about which the public has some substantial concern because it affects the welfare of citizens, or one to which considerable public notoriety or controversy has attached”... Public interest may be a function of the prominence of the person referred to in the communication, but mere curiosity or prurient interest is not enough. Some segment of the public must have a genuine stake in knowing about the matter published. <sup>8</sup> (#fn8)

With this in mind, the remainder of this paper canvasses the following mechanisms for enhancing control over one’s reputation online:

- A. De-indexing of search results;
- B. Removal/amendment of information at the source;
- C. The special case of youth
- D. Improving sites’ practices;
- E. Improving Education;
- F. Promoting further research ; and,
- G. Legislative solutions.

## A. De-Indexing

Perhaps the most frequently discussed means of improving individuals’ control over their online reputations has been “de-indexing.” De-indexing is the process by which a particular webpage, image, or other online resource is removed from the results returned by a search engine when an individual’s name is entered as the search term. It is important to note that de-indexing does not remove the content itself from the Internet, and does not prevent the content from being found through other search terms or by navigating the source website (for this reason, we use the term “de-index” rather than “take down” to refer to information being removed from search results). However, it does prevent the content from being linked prominently to an individual’s name in search results. As such, de-indexing can have an important impact on an individual’s reputation and right to privacy. <sup>9</sup> (#fn9)

As described in our [summary](#).

(/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/or\_intro/)

, while the majority of submissions felt that the parameters of the right to request de-indexing in the European Union can be problematic, it was argued (by some) that the privacy principles which underlie de-indexing are consistent with Canadian law. Providing an individual with some measure of control over personal information disseminated on the Internet (especially where it creates a risk of harm, or where there is no public interest in the information) is connected to fundamental values such as privacy, dignity and autonomy. <sup>10</sup> (#fn10) This measure of control can help individuals “move on from the past” <sup>11</sup> (#fn11) and reduces the potential for self-censorship of actions and statements. Implementing such control via de-indexing can strike an appropriate balance between privacy and freedom of expression (particularly as compared to, for instance, preventing or removing speech altogether).

In the analysis that follows, we do not seek to establish a new right or ability to request the de-indexing of search results; rather, we will examine whether such a measure exists under *current* Canadian law. To do this, we must answer two questions:

- Does [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) apply to the indexing of online content and display of search results by search engines?
- If so, in what circumstances, if any, does [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) require search engines to remove links in search results for searches of an individual’s name?

## *i) Search Engines Under PIPEDA (Personal Information Protection and Electronic Documents Act)*

First, we must clarify that the discussion that follows refers strictly to search engines' activity of indexing the web and generating search results based on that index. Many organizations that operate prominent search engines (Google, Microsoft, Yahoo, etc.) also have other business lines to which PIPEDA (Personal Information Protection and Electronic Documents Act) may or may not apply; they are not considered here.

With that note, we turn to the application of PIPEDA (Personal Information Protection and Electronic Documents Act) to search engines. Pursuant to paragraph 4(1)(a), PIPEDA (Personal Information Protection and Electronic Documents Act) applies to "every organization in respect of personal information that ... the organization collects, uses or discloses in the course of commercial activities."

In our view, by indexing webpages containing personal information, and returning links to those pages in search results, search engines are collecting, using and disclosing personal information within the meaning of PIPEDA (Personal Information Protection and Electronic Documents Act). When users search for information about an individual by name, search engines can create a detailed profile of all relevant information concerning that individual and return that information to the user. Search engines themselves acknowledge that their activities may involve personal information and they have policies to remove certain kinds of personal information, such as social insurance numbers, from their results.

Although most search engines are free, most also display advertisements alongside search results. The ability of search engines to sell this advertising space would not exist were it not for the search service they provide. The two functions have been described as "inextricably linked". <sup>12 (#fn12)</sup> Thus, there also seems little doubt that search engines collect, use and disclose personal information "in the course of commercial activities".

Some have argued that search engines are nevertheless exempt from PIPEDA (Personal Information Protection and Electronic Documents Act) because they serve a journalistic or literary function. <sup>13 (#fn13)</sup> However, search engines do not distinguish between journalistic/literary material. They return content in search results regardless of whether it is journalistic or literary in nature. We are therefore not convinced that search engines are acting for "journalistic" or "literary" purposes, or at least not exclusively for such purposes as required by paragraph 4(2)(c).

Some have also pointed out that it is unclear how certain requirements in PIPEDA (Personal Information Protection and Electronic Documents Act) can sensibly be applied to a search engine. For instance, as we noted in the OPC (Office of the Privacy Commissioner of Canada)'s Consent Report, <sup>14 (#fn14)</sup> 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. In our Consent Report, we recommend that Parliament consider new, properly framed exceptions to consent to deal with situations, such as the indexing activities of search engines, where consent may be impracticable, or where implied consent would be stretched to absurdity. We continue to believe that such clarification would be desirable.

In the meantime, we are of the view that the indexing of webpages and display of search results by search engines is captured by PIPEDA (Personal Information Protection and Electronic Documents Act). We must therefore apply the law as it stands to the best of our abilities. We will now turn to consider a search engine's obligations under the Act.

## *ii) What Do Search Engines Actually Do?*

For the analysis that follows, it is important to clarify the role of search engines. Search results do not simply and indiscriminately provide links to all web content associated with a search query. Rather, they are intended to provide users with results that a search engine considers *most relevant* to a user's search query.

For instance, we note that:

- Search results will often differ between users, based on what is considered 'most relevant' to him or her (personalized results).
- Websites that are considered "low quality" are regularly given diminished prominence in search results, or removed entirely.

- Search engines make efforts to ensure that “fake” news stories are flagged, defamatory search suggestions are removed, etc. <sup>15</sup>(#fn15)

In other words, search engines do not intend to simply create an index of what information exists online; rather, they seek to “provide people with access to relevant information from the most reliable sources available” <sup>16</sup>(#fn16).

Thus, with respect to searches for an individual’s name, search engines use personal (and non-personal) information to create a dynamic profile of what they consider to be the most “relevant” information available online which is available to be indexed in relation to that individual. <sup>17</sup>(#fn17)

### **iii) Search Engines’ Obligations under PIPEDA (Personal Information Protection and Electronic Documents Act)**

While organizations subject to PIPEDA (Personal Information Protection and Electronic Documents Act) are required to meet all obligations set out by the Act, in the context of de-indexing by search engines, the two most relevant provisions of PIPEDA (Personal Information Protection and Electronic Documents Act) are Principle 4.6 of Schedule 1 (and related provisions, such as 4.9.5 and 4.10) and subsection 5(3). We will discuss how each of these provisions apply to search engines’ activities in turn.

#### **Principle 4.6 – Accuracy (and related provisions)**

The principle pointing most directly to the right to de-index under PIPEDA is Principle 4.6 (and its related provisions under 4.9 and 4.10). This principle includes the following provisions related to the accuracy of personal information:

*4.6: Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.*

*4.6.1: The extent to which personal information shall be accurate, complete, and up-to-date will depend upon the use of the information, taking into account the interests of the individual. Information shall be sufficiently accurate, complete, and up-to-date to minimize the possibility that inappropriate information may be used to make a decision about the individual.*

*4.9: An individual shall be able to challenge the accuracy and completeness of [his or her personal information] and have it amended as appropriate.*

*4.9.5: When an individual successfully demonstrates the inaccuracy or incompleteness of personal information, the organization shall amend the information as required. Depending on the nature of the information challenged, amendment involves the correction, deletion, or addition of information.*

*4.10: An individual shall be able to address a challenge concerning compliance with the above principles to the [individual or individuals] accountable for the organization’s compliance.*

Search engines – as with any organization subject to PIPEDA (Personal Information Protection and Electronic Documents Act) – are required to meet their obligations under the Act. As previously established, the “use” to which search engines are putting personal information when results are returned on searches for an individual’s name is the creation of a “profile of the most relevant information” about that name that is available online – a profile that is the personal information of the individual. Search engines should, thus, be responsive to challenges that the profile presented in the form of search results is not accurate, complete, or up-to-date.

If an individual is able to successfully challenge the accuracy, completeness or currency (that is, the extent to which the information is up-to-date) of the results generated by a search for their name (because, for instance, the information at one or more of the returned results is demonstrably inaccurate, incomplete or up-to-date) then, per Principle 4.9.5, the results returned should be amended accordingly. The most obvious means to make such an amendment is to de-index the offending result and remove the link; however, in some situations, other solutions (such as lowering the ranking of a result, or flagging it as inaccurate or incomplete) may also be appropriate.

It will be important, though, to consider whether a successful challenge has been made out in light of Principle 4.6.1, which states that the extent of accuracy, completeness and currency required depends on purpose for which the information is to be used, and on the interests of the individual. For instance, a single inaccurate statement or the omission of a single fact, within an otherwise wholly accurate webpage, may not warrant de-indexing of the page – particularly where the inaccuracy or omission does not materially impact the interests of the individual. This must be considered on a case-by-case basis, and should take into account the public interest in the information remaining accessible.

### 5(3) – Appropriate purposes

Subsection 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act) states:

*An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate under the circumstances.*

Within the scheme of PIPEDA (Personal Information Protection and Electronic Documents Act), subsection 5(3) is “an overarching requirement” <sup>18</sup> (#fn18) that is superimposed on an organization’s other obligations to ensure that their purposes for collection, use and disclosure of personal information are limited to only those which a reasonable person would consider appropriate in the circumstances.

Generally speaking, we consider that search engines are using personal information for appropriate purposes when they index webpages containing personal information and return them in search results for searches of an individual’s name. Indeed, it is difficult to imagine successfully navigating the wealth of information online without the use of search engines. <sup>19</sup> (#fn19) This said, we are of the view that there are a certain number of limited circumstances in which a reasonable person would not consider it appropriate that specific content containing personal information is identified by a search engine as “relevant” in relation to a search of an individual’s name and given prominent placement in search results. These circumstances include, but are not limited to:

- Where that content is unlawful, or unlawfully published (e.g. where it contravenes a publication ban, is defamatory, or violates copyright; etc.) <sup>20</sup> (#fn20); and,
- Where the accessibility of the information may cause significant harm <sup>21</sup> (#fn21) to the individual, and there is either no public interest associated with the display of the search result, or the harm, considering its magnitude and likelihood of occurrence, outweighs any public interest.

As such, we consider that a search engine, once notified of one of the above circumstances by the individual whose personal information is at issue, should be required to remove the links to the content in question from its search results for searches performed on the individual’s name. These categories do not necessarily represent an exhaustive list of all such circumstances, for there may be others that emerge or evolve over time.

We are of the opinion that this represents an appropriate balance with freedom of expression, while having a significantly positive impact on an individual’s privacy rights. In particular, we note that in these scenarios a search engine’s actions do not remove the underlying content and do not affect its accessibility using other search terms. All that is removed is the link between the content in question and the individual’s name in search results. In the situations identified above, we consider that the limited prejudicial effects on access to the information in question are clearly outweighed by the beneficial impacts that removing the links in search results can have on the individual’s privacy and dignity.

### Factors relevant to assessing the public interest

We have stated that the public interest in information remaining available is a relevant consideration in evaluating de-indexing requests under either subsection 5(3) or Principle 4.6. Among the factors which in our view could be relevant to assessing whether there is a public interest in the information remaining accessible in the context of a de-indexing request are:

- whether the individual concerned is a public figure (e.g. a public office holder, a politician, a prominent business person);
- whether the information at issue relates to a matter of public controversy or debate;
- whether the information relates to an individual's private life as opposed to, for example, their professional or working life;
- whether the information concerns a criminal offence for which the individual has been given a discharge, a pardon, or a record suspension; and,
- whether the information relates to a minor (see section on Youth below).

The first two factors point towards a public interest in the information remaining accessible, whereas the last three may suggest the opposite. This list is of course not exhaustive. There may be other circumstances that are relevant to a particular case, and not all of the above factors may be relevant in any given situation. Ultimately, the overarching consideration is whether the public has a legitimate interest in accessing the information at issue.

A final point to emphasize is that the evaluation must be done in the specific context of a de-indexing request. In other words, the question is not whether the underlying information serves the public interest in the abstract, but whether its continued availability in search results for searches of an individual's name is in the public interest.

#### *iv) Critiques with respect to de-indexing*

Based on the above analysis of search engines' obligations under PIPEDA (Personal Information Protection and Electronic Documents Act), we are of the view that, individuals should be provided the ability to request the de-indexing of search results, and that there are some circumstances under which these requests should be honoured. In our view, our interpretation of the law strikes an appropriate balance between individuals' privacy interests and the right to freedom of expression. However, we recognize a number of submissions to our consultation raised legitimate critiques about a right of individuals to request the de-indexing of search results. In this section, we discuss (and, to the extent possible, address) a number of them.

##### *a) Effectiveness of de-indexing*

Some have argued that de-indexing is an ineffective remedy, since the underlying content remains available online. In our Office's experience from past investigations, there is a difference between having information available to those who explicitly seek it out directly from source websites for specific purposes (for example, a lawyer doing jurisprudential research in CanLII (Canadian Legal Information Institute) or a journalist seeking out past articles on a given issue), and, the same information being "stumbled upon" or "fished out" by a snooping friend, colleague, neighbor or other acquaintance through a simple query search by an individual's name. <sup>22 (#fn22)</sup> The OPC (Office of the Privacy Commissioner of Canada) believes that removal of links from search results in the limited circumstances identified above will have a significantly positive impact, even where the source information remains.

##### *b) Role of the Private Sector in the Balancing of Rights*

In submissions, it was suggested that it is inappropriate for a private sector organization to make decisions balancing privacy rights against the right to expression.

While this is a legitimate concern we also note that organizations do regularly engage in such balancing to some extent— for instance, in establishing terms of service which may result in content, statements or even entire accounts being removed. Search engines, in particular, already have in place mechanisms to consider de-indexing requests and remove content which is potentially harmful (e.g. credit card numbers; images of signatures) or illegal (e.g. copyright infringement) from their search results.

We also note that the organization's role as an initial responder is in fact mandated under PIPEDA (Personal Information Protection and Electronic Documents Act) Principle 4.10.2, which states:

*Organizations shall put procedures in place to receive and respond to complaints or inquiries about their policies and practices relating to the handling of personal information. The complaint procedures should be easily accessible and simple to use.*

Search engines are therefore responsible for addressing requests to de-index results in accordance with their legal obligations under PIPEDA (Personal Information Protection and Electronic Documents Act).

Beyond this, it is important to note that search engines have created the situation in which content is so readily linked to an individual's name and are actively perfecting algorithms to personalize search results over time as part of their business model.

Some have suggested that de-indexing requests should only be considered by an oversight body or a court given the fundamental rights at stake. While individuals and search engines should ultimately have access to review by an independent arbiter in contested cases, we consider it appropriate to have search engines providing the first level of review of a de-indexing request. Indeed, having search engines initially assess de-indexing requests arguably promotes, rather than hinders, access to justice and the rule of law by providing a practical and expedient remedy for individuals. <sup>23</sup> (#fn23)

Nonetheless, we recognize the legitimacy of the concerns raised with respect to the role of the private sector in balancing rights. As such, this is an area which is worthy of future consideration.

Lastly, while we believe it is reasonable for search engines to assume this first level of responsibility, they are welcome to engage with regulators (and/or other relevant stakeholders) in the development of their de-indexing request assessment process.

### ***c) Notification to Publishers***

Related to the issue of balancing of rights, above, some submissions have raised the issue that the de-indexing procedure established in the EU (European Union) is one-sided: de-indexing requesters are able to make their case for the removal, but there is no equivalent party arguing for the public interest in retention of the search result. European regulators tend to recommend against, as a general practice, notifying the source website of the de-indexing request, though recognizing that making contact with the original publisher may be appropriate in some circumstances (such as "in particularly hard cases"). <sup>24</sup> (#fn24)

In addressing this issue, we are cognizant of both the operational and logistical challenges that would be associated with any requirement for a search engine to engage with the source of information subject to a de-indexing request, and the fact that de-indexing as a means of establishing control over one's reputation would become meaningless, or even harmful, if de-indexing requests became prominently known.

It must also be emphasized again that de-indexing in this context does not remove the source content from the web and only removes links to the source content from search results for searches on an individual's name. Thus, the impact of de-indexing on source websites will, in many cases, be minimal.

This said, we recognize that there may be some cases where a search engine may consider it helpful to obtain input from the source website prior to making a decision on a de-indexing request or to allow a source website to object to a decision to de-index after the fact. Ultimately, we leave it to search engines to devise mechanisms that are appropriate; however, we flag this as a procedural issue which is deserving of further consideration. -

### ***d) Burden on search engines***

In submissions, it was also suggested that to establish and operate processes to adjudicate de-indexing requests was too high of a burden to place on search engines, and may hamper competition.

We acknowledge that the establishing and operation of a mechanism to handle takedown requests is not an insignificant cost. However, setting aside that all organizations are required under PIPEDA (Personal Information Protection and Electronic Documents Act) to “put procedures in place to receive and respond to complaints” <sup>25</sup> (#fn25), search engines are in the business of making information more accessible, and, in the cases of the most widely used search engines, they generate substantial revenue from doing so; it does not seem unreasonable that this would engender an obligation to address any inappropriate or harmful impacts caused by their own actions.

As stated prior, at minimum we believe that Canadians should be provided a mechanism to challenge compliance with PIPEDA (Personal Information Protection and Electronic Documents Act) with respect to information returned in search results, based on the obligations described above.

### *e) Territorial Scope*

The appropriate territorial scope of de-indexing is an on-going global debate. As a guiding principle, the OPC (Office of the Privacy Commissioner of Canada) is of the position that de-indexing based on PIPEDA (Personal Information Protection and Electronic Documents Act) should be effective in order to be meaningful, but also limited in order to respect other jurisdictions’ authorities. We do not believe that de-indexing results from searches made on the Canadian domain for a search engine (e.g. “google.ca”) is sufficient as the information will still remain easily accessible via the .com or country-specific domains. However, we also believe that de-indexing results globally could potentially unduly interfere with the sovereignty of other countries. In order to ensure that the protections afforded by PIPEDA (Personal Information Protection and Electronic Documents Act) to individuals are effective yet do not impermissibly extend beyond Canada, we believe that geo-fencing techniques should be applied so that de-indexing of search results is limited to searches originating from within Canada. <sup>26</sup> (#fn26)

While an admittedly imperfect solution, we believe that for now, geo-fencing strikes the appropriate balance between effectiveness and appropriate territorial scope. We may revisit this position as Canadian and international law evolves.

### *v) Concluding note*

De-indexing is a means of providing an *effective* remedy to individuals for certain privacy harms, but it is not without challenges and is not a perfect remedy for all harms to online reputation. We have taken the position that PIPEDA (Personal Information Protection and Electronic Documents Act) requires organizations, including search engines, to assume accountability for their actions, and provide some challenge-type mechanism that individuals can resort to when challenging compliance with relevant principles. We believe that the position set out above strikes a fair balance and is workable. Furthermore, we are of the view that, based on the current law, it is appropriate to take action given the significant privacy interests at stake. However, we recognize that submitters to our consultation have raised legitimate concerns about the impacts of such a mechanism on, among other things, rights, such as freedom of expression. These concerns, along with those noted immediately above, are worthy of further consideration. We would therefore recommend that Parliament also undertake a full examination of this issue to determine whether we have struck the right balance. We discuss this further in Section G of this paper.

## **B. Source Amendment/Takedown**

Whereas de-indexing allows information to remain online (though breaking the immediate link between it and the individual), amendment/takedown at the source modifies or removes the information entirely. This is clearly a stronger privacy protection, but in at least some circumstances it can pose much greater challenge with respect to freedom of expression.

In examining the possibility of source amendment/takedown, we examine two different scenarios: (i) where the information in question was supplied by the individual him/herself; and, (ii) where the information was supplied by a source other than the individual to whom the information relates.

## *Self-provided information*

PIPEDA (Personal Information Protection and Electronic Documents Act) provides individuals the right to withdraw consent subject to legal or contractual restrictions (Principle 4.3.8), and requires that personal information that is no longer needed be destroyed, erased or made anonymous (Principle 4.5.3).

Taken together, these two principles imply that individuals should be provided the ability to remove information which they themselves have provided to an online forum that is involved in commercial activity (including, but not limited to, a social network). To the extent possible, this ability should be: (i) granular, (ii) self-directed, and (iii) effective. For instance, individuals should be able to delete one or more social media posts without having to delete their entire account, and they should be able to do so independently, without having to make a request subject to the organization's response. Many social media sites (and other similar services) already offer such an ability, but as described in a [submission](#)

(/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub\_or\_09/)

, the quality and accessibility of takedown tools varies significantly.

This ability to delete self-posted information should be near-absolute, except to the extent that it is subject to legal or contractual restrictions. In particular, we do not believe that this ability should be subject to a public interest test; individuals should be able to delete information they have posted about themselves regardless of whether others would prefer it remain available.

It is worth noting that this ability to delete self-posted information applies only to the initial post; the situation in which other individuals have captured that information and re-posted it is discussed below.

## *Information provided by others*

Where personal information is provided to an organization by someone other than the subject (including where information posted by the individual is re-posted by another person), under PIPEDA (Personal Information Protection and Electronic Documents Act) individuals do not have an unqualified right to remove that content.

This said, there are at least two principles of PIPEDA (Personal Information Protection and Electronic Documents Act) <sup>27</sup> (#fn27) under which an individual can at least challenge information posted about them by another individual: accuracy and appropriateness.

As stated prior, Principle 4.9.5 creates an obligation for organizations to amend information that is demonstrated to be incomplete, inaccurate or not up-to-date. Thus, at minimum, where personal information is provided to an organization acting in the course of commercial activity by someone other than the individual to whom the information relates, the individual should be provided a mechanism by which demonstrably inaccurate, incomplete or out of date information can be challenged and amended. This is particularly the case where the organization is creating a profile of the individual based on information provided by others which is intended to allow for decisions to be made about the individual. In our view, correction, removal or other amendment to demonstrably inaccurate, incomplete or out of date information represents an appropriate balance with freedom of expression.

Accordingly, an individual should be able to challenge the accuracy, completeness, and currency of the posted information and the source website or social media platform (if commercial) should have a mechanism in place to provide an adequate response.

As well, subsection 5(3) – which requires personal information only be collected, used and disclosed for purposes that a reasonable person would consider appropriate under the circumstances – may also operate to require organizations to remove content posted by others in respect of an individual. For instance, in our guidance on [no-go zones](#) (/en/privacy-topics/collecting-personal-information/consent/gd\_53\_201805/), we take the position that purposes that are otherwise illegal, and the soliciting and posting of personal information for the purpose of incentivizing payment for its removal, would be considered inappropriate under subsection 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act).

## C. The special case of youth

As described in our discussion paper, maintaining one's online reputation poses a particular challenge for children and teens. They often have little or no option but to engage online (e.g. due to social pressures or requirements placed on them by schools). They are also in a time of experimentation, in which boundaries are being tested. It is thus critical that youth be provided with a means of reinventing themselves as they mature and enter adulthood – a fact recognized by the existence of “clean slate” and other protective mechanisms in Canada and elsewhere. <sup>28</sup> (#fn28)

In *A.B. v. Bragg*, the Supreme Court recognized the special case of youth when it comes to privacy protection <sup>29</sup> (#fn29).

Recognition of the *inherent* vulnerability of children has consistent and deep roots in Canadian law. This results in protection for young people's privacy under the *Criminal Code ... Youth Criminal Justice Act, ...* and child welfare legislation, not to mention international protections such as the *Convention on the Rights of the Child, ...* all based on age, not the sensitivity of the particular child. [emphasis in original]

Alongside this inherent vulnerability, there is a recognition that the cognitive and emotional maturity level of children and youth is undergoing constant development, and that particular consideration should be provided to them. For instance, in our recent consent report, the OPC (Office of the Privacy Commissioner of Canada) took the position that, save for exceptional circumstances, consent for the collection, use and disclosure of personal information of children under the age of 13 must be obtained from their parents or guardians. For youth aged 13 to 18, consent can only be considered meaningful if organizations have taken into account their level of maturity in developing their consent processes and adapted them accordingly.

Building on this position, we propose a number of additional measures for protecting the online reputation of children and youth. First, where subsection 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act) is being evaluated in the case of children or youth (either for the purposes of de-indexing search results or removing source content), consideration should typically weigh more heavily in favour of de-indexing or removal of the content. Second, in the case of information provided to an organization or otherwise posted by youth about themselves, the right to removal should be as close to absolute as possible, and unfettered by any contractual limitations. Parliament should consider formally enshrining such a right in statute as exists in other jurisdictions.

Finally, in the current social media age, we note that it is not uncommon for information about children and youth to be posted by their parents. A “cute” anecdote or photo may – at the time, or in the future - be highly embarrassing or even harmful to the child or youth, and youth have indicated a desire for greater control of this information. <sup>30</sup> (#fn30) Thus, we recommend that Parliament also consider providing youth with some ability, upon reaching the age of majority, to request and obtain removal of online information posted about them by their parents or guardians who until then had substitute decision-making power. Such an ability will, of course, need to be crafted in such a way as to be practical and respect the expressive rights of the parent.

## D. Improving Sites' Practices

In addition to ensuring appropriate measures exist to enable individuals to control information about them, organizations also play a key role in creating an environment which limits the potential for reputational damage. To paraphrase a response

(/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub\_or\_04/)

to our discussion paper:

“[P]olicymakers should give [users] a break and pay more attention to corporate practices and policies that compromise their ability to negotiate privacy in networked spaces.”

The organizations which operate online services make frequent decisions about the incentives individuals have to share personal information (and the level of detail and sensitivity of information being shared) and the frequency with which individuals are presented with prompts related to privacy (e.g. controls over the visibility of *all* posts vs. controls over individual posts). These organizations are also able to create community standards with respect to the non-tolerance of abuse, and mechanisms by which individuals are encouraged to resolve disputes within the community (rather than needing to resort to an overseer or regulator). The organizations also make choices with respect to reputation control mechanisms, such as takedown mechanisms and the amount of time for which information is both retained and easily accessed.

All of these decisions, and the way that they are implemented and communicated <sup>31</sup> (#fn31), have significant impacts on individuals – both directly, by allowing them to exercise self-responsibility, and indirectly, by creating an environment that lessens the likelihood of harms.

To the extent that the design decisions listed above relate to obligations under PIPEDA (Personal Information Protection and Electronic Documents Act), we will seek to provide advice to organizations, and will encourage industry to develop codes of practice in some key areas. <sup>32</sup> (#fn32) In particular, it is recommended that organizations coordinate the development of an industry-wide Code of Practice related to information takedown policies, privacy defaults and procedures. At a minimum, such a Code would respect and implement the relevant “no-go zones” that the OPC (Office of the Privacy Commissioner of Canada) has identified in its guidance and uphold de-indexing or take-down requests in the additional circumstances identified above. Ideally, such a Code would, over time, establish a reasonably consistent experience that would allow Canadians to understand the basis by which organizations are making decisions with respect to their de-indexing or takedowns requests.

Lastly, we note that the OPC (Office of the Privacy Commissioner of Canada) has clearly indicated its intention to take a more proactive role in ensuring compliance with PIPEDA (Personal Information Protection and Electronic Documents Act), to address broader, systemic privacy risks to Canadians. This will be of particular importance in the realm of Online Reputation, given the number of individuals who may be impacted by a single non-compliant organization, and the significant impacts on individuals that can result from non-compliance, particularly the disproportionate impact on vulnerable individuals, who may opt not to file complaints to our Office in order not to bring further attention to themselves, or open themselves to retribution. Each of these factors point to the benefits of curbing privacy risks up front, before problems occur, or in high-risk areas where problems may not be outwardly detectable.

In summary, the OPC (Office of the Privacy Commissioner of Canada) does not see the burden of protecting reputation resting solely with individuals. Organizations have a role to play, and the OPC (Office of the Privacy Commissioner of Canada) will continue to proactively seek opportunities to ensure this role is filled.

## E. Improving Education

Next, the need for continued education on privacy is obvious. In our consent report, we stated that:

*In terms of public education, the most effective strategy may well be to teach children about privacy at an early age. We therefore urge provincial and territorial governments to integrate privacy education into school curricula.*

Internationally, we helped develop the 2016 Marrakech Resolution (<https://icdppc.org/wp-content/uploads/2015/02/Resolution-2016-on-Privacy-education.pdf>) calling for the adoption of a competency framework for privacy education in schools

(<https://icdppc.org/wp-content/uploads/2015/02/International-Competency-Framework-for-school-students-on-data-protection-and-privacy.pdf>)

. Currently we are participating, through the International Working Group on Digital Education, in efforts to further the inclusion of privacy and data protection skills in the education of students around the world.

In general, we are in agreement with the British Columbia Freedom of Information and Protection Association, which stated in its submission <sup>33</sup> (#fn33):

*Public education that takes a rights-based approach to online reputation can help reinforce norms that protect online reputation, in addition to spreading knowledge of the law, how to make use of architecture-based controls, and how to evaluate protections offered across a multitude of platforms.*

Privacy education should serve to develop good online citizens, armed with the technical knowledge of how to protect themselves and a strong sense of how and why to act responsibly online. To advance this, a number of topics have been identified as potential points of focus, including:

- Educating individuals on currently available mechanisms to control reputation (takedown mechanisms, privacy settings) and emerging privacy enhancing technologies; and,
- Ensuring that educational messaging includes additional emphasis on the importance of thinking about the potential impacts of one's actions on *all* relevant parties.

Education may also be an important element to some of the solutions presented previously in this paper – for instance, it should be made clear to Canadians that, in many (or most) cases, search results do not present a complete picture of an individual (only the information online about him or her). Thus, it should not be assumed that a decision made based on search results is a decision made on complete information.

Many stakeholder groups have offered to work with the OPC (Office of the Privacy Commissioner of Canada) on the development and distribution of educational materials and we will continue to engage with these groups where appropriate. The OPC (Office of the Privacy Commissioner of Canada) – along with its provincial and territorial counterparts – have also sent a joint letter ([/en/opc-news/news-and-announcements/2017/let\\_171103/](/en/opc-news/news-and-announcements/2017/let_171103/)) to the Canadian Council of Ministers of Education calling for privacy protection to be incorporated into curriculum for digital education.

Lastly, as mentioned in the previous section, we will work with organizations to ensure that individuals have meaningful opportunities to exercise the learnings from this educational material.

## F. Promoting further research

As recommended by a number of submissions, the OPC (Office of the Privacy Commissioner of Canada) will continue to research and consult on youth norms, attitudes and challenges with respect to reputational privacy in order to better understand and make recommendations with respect to what practices are appropriate for sites and online services aimed at young Canadians. We will also continue to solicit information about what measures may be needed, or how existing measures can be adapted, to address the reputational challenges faced by those groups that have been disproportionately targeted for, and impacted by, online abuse, such as women.

Individual online services have a responsibility to provide appropriate options and controls to their users; however, there is also benefit to the widespread availability and adoption of services and technologies for managing online reputation that are independent of any particular website. Similar to what we noted in our consent report, we believe that there is no shortage of technologies or good ideas for protecting online reputation; they have simply not been sufficiently developed and/or adopted.

As such, we will encourage research, development and adoption of new solutions for protecting online reputation. In particular, we invite proposals under our Contribution Program to research and develop new solutions for protecting online reputation, and we have included a special call for privacy enhancing technologies, or PETs, in the 2018-19 version of the Program.

## G. Legislative solutions

Throughout this position paper, we have generally proposed solutions to the challenges associated with online reputation which the OPC (Office of the Privacy Commissioner of Canada) and organizations can undertake given current authorities. However, there are also a number of matters which we believe should be considered by Parliament.

First, as discussed in the section on “De-Indexing,” the OPC (Office of the Privacy Commissioner of Canada) is of the opinion that the position set out in this paper is workable, appropriately balances important rights and interests, and is supported by PIPEDA (Personal Information Protection and Electronic Documents Act). However, we acknowledge that this position clearly raises issues around the balance of an individual’s right to privacy with the right to free expression, as well as around the appropriate role of private sector stakeholders in assessing this balance. It would be inappropriate for the OPC (Office of the Privacy Commissioner of Canada) not to act on this issue – we must apply PIPEDA (Personal Information Protection and Electronic Documents Act) to the best of our ability and understanding, attempting to strike the appropriate balance. However, we also believe that it is important for Parliament to consider this issue, looking at the concerns raised in this paper as well as external factors, such as the impacts any differences between the Canadian and European legislative frameworks with respect to individuals’ control of online information may have on adequacy.

Next, there are opportunities to generally enhance the OPC (Office of the Privacy Commissioner of Canada)’s powers to include stronger enforcement mechanisms, and enhanced ability to act proactively, under PIPEDA (Personal Information Protection and Electronic Documents Act). In our consent paper, the OPC (Office of the Privacy Commissioner of Canada) has called for order-making and fining powers, as well as more formalized powers to act proactively (including by requiring organizations to demonstrate accountability). The rationale and conclusions presented in that paper apply equally here. By way of example, we believe it would be of significant benefit for the OPC (Office of the Privacy Commissioner of Canada) to be able to proactively examine how organizations are responding to the de-indexing requests and challenges to accuracy described above.

Beyond this, there are also opportunities to either clarify or strengthen the mechanisms available to individuals. To recap, these include:

- Clarifying the application of certain aspects of PIPEDA (Personal Information Protection and Electronic Documents Act) to search engines, perhaps by establishing a new, limited exception to consent as described in our Consent report;
- Establishing a stronger ability for youth to request and obtain the deletion of information they have themselves posted on social media, and in appropriate cases, information posted about them online by their parents or guardians when they reach the age of majority.

Lastly, a number of submissions spoke to the notion of “specific legislation” to address particular challenges related to reputation. We agree that if it becomes clear that a particular collection, use or disclosure of personal information is highly offensive to Canadians, Parliament should consider formalizing restrictions or prohibitions of that activity (such as has been done for non-consensual distribution of intimate images). This option will also be beneficial for addressing the challenges posed by the person-to-person interactions that can be extremely harmful, but which are outside PIPEDA (Personal Information Protection and Electronic Documents Act)’s reach and not covered by existing criminal laws.

## Conclusion and next steps

During the OPC (Office of the Privacy Commissioner of Canada)'s 2015 Priority Setting Exercise, we heard from stakeholders and the Canadian public that while they recognize the personal and professional benefits of participating in the online world, they are increasingly concerned about their online reputation. The consultation paper that followed it aimed to start a discussion about potential ways to address issues associated with the permanency of personal information online and the effect on reputation.

We believe that the measures outlined above represent a significant step toward achieving our goal of helping to create an environment where individuals may use the Internet to explore their interests and develop as persons without fear that their digital trace will lead to unfair treatment. The position is being put forward as a draft, for consultation. Following a consultation period on this position paper, we will finalize our position and develop an Action Plan that will put these new measures into practice. We look forward to working with a broad range of stakeholders to bring in a new age of online reputation for Canadians.

---

## Notes

- 1 *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 SCR 927, p. 969.
- 2 *Ford v. Quebec (Attorney General)*, [1988] 2 SCR 712 at para. 59.
- 3 *Edmonton Journal v. Alberta (Attorney General)*, [1989] 2 SCR 1326, pp. 1339-1340; *R. v. National Post*, [2010] 1 SCR 477 at para. 28.
- 4 *Aubry v. Éditions Vice-Versa inc.*, [1998] 1 SCR 591 at para. 62.
- 5 *Hill v. Church of Scientology of Toronto*, [1995] 2 SCR 1130, at para. 121 (“*Hill*”).
- 6 *Hill, ibid.* at para. 107-108.
- 7 *Grant v. Torstar Corp.* [2009] 3 SCR 640, para 51.
- 8 *Grant v. Torstar Corp.*, [2009] 3 SCR 640 at para. 105, citing Raymond E. Brown, *The Law of Defamation in Canada*, vols. 2-4, 2nd ed. Scarborough, Ont.: Carswell, 1999 (loose-leaf updated 2008, release 3), at pp. 15-137 and 15-138.
- 9 In other jurisdictions – the European Union (EU), in particular – this has been referred to by some as the “Right to be Forgotten.” We have used the term “de-indexing” instead as it is more precise in this context. The “right to be forgotten” can encompass more than just de-indexing of search results. This said, we acknowledge that the proposals contained in this position paper, taken together, have some similarities to the EU (European Union) General Data Protection Regulation (GDPR)'s “Right to Erasure (‘Right to be forgotten’).”
- 10 Gratton/Polonetsky.
- 11 Korenhof & Gorzeman, as cited in Gratton/Polonetsky.
- 12 *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063, at para. 60, aff'd 2015 BCCA 265, 2017 SCC 34.
- 13 PIPEDA (Personal Information Protection and Electronic Documents Act), s. 4(2)(c).
- 14 OPC (Office of the Privacy Commissioner of Canada)'s Consent Report

- 15 [Google – "Our latest quality improvements for Search"; Bing adds Fact Check label in SERP to support the ClaimReview markup](#)
- 16 [Google – "Our latest quality improvements for Search"](#)
- 17 To be clear, we assert that search engines create a profile of *information about* the individual, not a profile of the individual.
- 18 *A.T. v. Globe24h.com*, 2017 FC 114, paragraph 73 ("*Globe24h.com*").
- 19 See e.g. *Niemela v. Malamas*, 2015 BCSC 1024, at para. 102: "There are hundreds of millions of active websites over the Internet and trillions of webpages. Search engines make the Internet a viable and effective information and communication resource. The Internet cannot be successfully navigated without search services such as those Google provides. If hyperlinks are the pathways search engines are the maps."
- 20 See, for instance, *Google Inc. v. Equustek Solutions Inc.*, 2017 SCC 34.
- 21 As defined in section 10.1(7) of [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) (not yet in force).
- 22 For instance, in the *Globe24h.com* matter, complainants to our office were not primarily concerned that their sensitive personal information existed in court and tribunal decisions published online. They were concerned when those decisions were copied and reposted in a manner that made them accessible through searches for their names in search engines: see *A.T. v. Globe24h.com*, 2017 FC 114.
- 23 As raised in the [submission](#) by Avner Levin. Submissions by [Bricker et al.](#), and Gratton & Polonetsky also recognize the need for a "simpler, cheaper and faster process" for processing de-indexing requests, suggesting that the current model (obtaining a Report of Findings from the [OPC \(Office of the Privacy Commissioner of Canada\)](#) and, if necessary, bringing an action to Federal Court) would not suffice.
- 24 See, for instance, Article 29 Working Party [Guidelines](#) on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain ...", para. 23.
- 25 Principle 4.10.2.
- 26 Geo-fencing could be accomplished, for instance, by limiting any de-indexing to searches performed from a Canadian IP address.
- 27 Assuming [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#) applies. Personal information that is collected, used or disclosed by an individual for personal or domestic (and no other) purposes will be outside the scope of [PIPEDA \(Personal Information Protection and Electronic Documents Act\)](#): see s. 4(2)(b).
- 28 This includes laws such as Canada's *Youth Criminal Justice Act* (which prevents publication of the names of youth offenders, and limits access to youth records) and newer laws aimed at the online environment such as California's *Privacy Rights for California Minors in the Digital World*, which allows youth to remove or obtain removal of any information provided to a website, app or online service.
- 29 *A.B. v. Bragg Communications Inc.*, 2012 SCC 46, [2012] 2 S.C.R. 567, para. 17.

- 30 See, for instance, Moser, C., Chen, T., and Schoenebeck, S. "Parents' and Childrens' Preferences about Parents Sharing about Children on Social Media." CHI 2017, May 06 - 11, 2017, Denver, CO, USA.
- 31 For example, see the OPC (Office of the Privacy Commissioner of Canada)'s updated Guidelines for Online Consent, which puts an increased responsibility on organizations to show that they have communicated relevant information to users in a meaningful, accessible manner.
- 32 Where these design decisions do not strictly fall under PIPEDA (Personal Information Protection and Electronic Documents Act) – such as the use of peer-to-peer dispute resolution mechanisms – we will seek to understand, and educate organizations about, their impacts on Canadians.
- 33 British Columbia Freedom of Information and Privacy Association.
- 

**Date modified:**

2018-01-26