February 12, 2018

# A Right to be Forgotten Online: A Response to the Office of the Privacy Commissioner Draft Position

**By:** Emily Laidlaw

**Document Commented On:** Draft OPC Position on Online Reputation

The Office of the Privacy Commissioner (OPC) published its draft position on online reputation last week stating that the *Personal Information Protection and Electronic Documents Act*, SC 2000, c-5 (PIPEDA) provides a right to de-index search results (remove a link to a webpage from search results based on a keyword search) and a right to source takedown (removal of a webpage from the host site). De-indexing and source takedown are specific ways that a person might deploy a right to be forgotten, an issue hotly debated for several years, but especially since the Court of Justice of the European Union decided *Google Spain SL, Google Inc v Agencia Espanola de Proeccion de Datos (AEPD), Marios Costeja Gonzalez*, (2014) Case C-131/12 (known as *Google Spain*). Scholars have already responded to the OPC, such as here, here and here. I offer a different commentary, reflecting my first critical thoughts on three key issues arising from the report: (a) the public interest test suggested by the OPC to balance freedom of expression and privacy; (b) the role of private technology companies; and (c) the blurring of the line between data protection and defamation regimes. While I will discuss source takedown briefly (and for a more thorough analysis of intermediary liability and defamation law, see my work with Dr. Hilary Young here), the focus in this post will largely be on search results.

This idea of the right to be forgotten – that you can craft the story that is written about you on search results – at its core is a question of who controls your public narrative. It is both deeply personal and public relations maneuvering. The OPC's report illustrates how difficult it is to finely balance the various interests at stake. For years when my name was inputted in Google the first result was a rather dismal time from a 10km race I participated in (if I had known this would leave such a digital imprint I would have run a lot faster). Now, thankfully, searching my name reveals largely professional links, to my work, publications and interviews with the media. I have not, as of yet (knock on wood), been slaughtered online in a way that appears in search results, and certainly not in the first page of results (which matters when 91.5% of users view the first page of search results, but only 4.8% view the second page of results). That is not the story for many people.

The victims range from law students excoriated online (see the case of auto-admit involving Yale law students), professionals and businesses rated poorly (RateMDs.com, RatemyProfessors.com, RipoffReport.com, TripAdvisor.com, to name a few), to children in embarrassing photos or videos (remember the treatment of Star Wars boy), to people targeted for abuse (consider revenge pornography or similar). Some of the results returned are incomplete, such as listing a charge but not a dismissal of the charge. In the case of *Google Spain*, the information was out-of-

date, an old newspaper report detailing a bankruptcy. Everyone is vulnerable, although studies show that if the content created arises from online harassment, traditionally marginalized groups are especially vulnerable (see, for example, here). Is Google posting the comments? No. Google is, however, indexing these links in a searchable online library. Google does remove content for policy reasons (e.g. revenge pornography) or with a court order. All of this matters for the person seeking a new job (although see here), for outliving your past, for correcting lies and for owning your life story. The thorn is that you don't own your life story, not really. People write reviews of services, and should be allowed to do so. People get caught up in stories of public interest (whether because they are public figures or not). These social interactions have positive impacts too – vouching for the quality of services and products. We instinctively can see differences between these stories, but it is more difficult to articulate a workable benchmark for what belongs and does not belong in the public narrative of our lives.

**Overview**

Recall that the OPC's role is limited here to the framework of PIPEDA, which is a narrow piece of data protection legislation that obligates organizations that collect, use and/or disclose data to abide by certain principles, namely that it is appropriate, complete, accurate and current. In this report the OPC interprets PIPEDA to mean that individuals can challenge indexing of certain webpages on those bases. The solution might be to de-index the webpage, although at times, lowering the link in search rankings might be sufficient. There are limits. A single inaccuracy in an otherwise accurate article might not result in de-indexing, and the de-indexing would be limited to results returned from searching an individual's name, not the myriad of other searches that might reveal information about a person (see Michael Geist's comment on this issue).

Along the same lines, individuals would have a near-absolute right to withdraw consent for information they have posted online, requiring websites to then destroy, erase or anonymize information that is no longer needed. This is trickier if an individual is the subject of information posted by a third party, in which case the right is more limited to information that is inappropriate, inaccurate, incomplete or out-of-date.

Sound good? The problem is that, as drafted, it is unworkable. It is, however, a good place to start an important conversation concerning the meaning of reputation in the digital age, one that will take longer than the public consultation sought by the OPC. Ultimately, the efforts of the OPC highlight the limits of the OPC's power, and the need to revamp the system of privacy protection in Canada in light of technology, which requires both re-imagining of protection of reputation and how to resolve disputes. I do not wish to dissuade the OPC from tackling online reputation, but rather warn that it requires more stakeholders involved, greater government attention, and at minimum significant amendments to the current draft proposal. We should also not be complacent to think this proposal answers the larger issues we face concerning online reputation.

There are some key strengths in the draft report that are not discussed in this post, which focuses on the more contentious issues. I welcome the OPC's strong stance on protection of youth, giving them a near-absolute right to remove posts or information they have provided to an

organization, including being able to seek removal of information posted by their parents (Facebook using parents take note) and improving privacy education.

**Balancing Freedom of Expression and Privacy: The Public Interest Test**

In order to give effect to a right to be forgotten an assessment must be made of the content in question, which requires the right to freedom of expression to be balanced against privacy. How do you balance a claim that the content linked from a search result is inaccurate or incomplete against the right to free speech? In the OPC's view, "this balance can be best achieved in the context of online reputation by considering whether the accessibility of personal information is in the public interest." What this means is that if an individual challenges content under PIPEDA, the only way that the information will remain accessible is if it is speech in the public interest, a troublingly high threshold for free expression.

I understand the draw of such an approach. It provides a solution to the problem that one's public narrative is not entirely under their control. However, this sets the bar too high. Suddenly, accessing un-curated information will only be for content in the public interest – a difficult concept to pin down at the best of times by a court, but made all the more difficult when it is being assessed and acted on by the first responders, namely search providers, social networking providers etc. In defamation law, the question of whether a publication is a matter of public interest enters the analysis when exploring the defences of fair comment, responsible journalism or qualified privilege. Certain failures by the author might be forgiven if the subject matter was of sufficient public interest, namely that it is something on 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" (*Grant v Torstar*, 2009 SCC 61 (CanLII) at para 105). This concept does not translate easily to the data protection context. What kind of inaccurate, incomplete or out-of-date information would be spared de-indexing because it was of public interest? In defamation, for example, a responsible journalist might have a defence where he/she made an inaccurate statement in an otherwise solid article in the public interest as long as not motivated by malice. This does not translate seamlessly to the obligations of organizations that gather, use or disclose data commercially.

The OPC identifies several factors to take into account in assessing public interest, although it is not an exhaustive list (below verbatim):

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

Is a bad review on RateMDs in the public interest? It does not involve a public figure or a matter of public controversy, but it does involve a professional. Assuming the review can be assessed for accuracy by a content moderator (and these types of reviews are particularly difficult for moderators to assess), then the public interest would play little role in the analysis and if the information is found to be inaccurate then it would be de-indexed. What about someone caught up in an online shaming? Many subject to it consider their statements or actions to have been taken out of context, arguably spun in a way that was inaccurate. The answer by those doling out the shaming is often that this is something the individual deserved for behaving badly – a reckoning. In their minds, this would be a matter of public concern or controversy. This begs the question, what is the public interest litmus test for indexing online commentary?

Of course, public interest is not the only test for de-indexing. The information would have to meet the criteria under PIPEDA, namely that it is inappropriate, inaccurate, incomplete or out-of-date. The problem is that much of the content at issue is notoriously difficult to assess on those criteria, with the exception of things like sexually explicit images. Consider accuracy or appropriateness (with the OPC advising that defamatory content, among others, is unlawful and therefore inappropriate to index). A recent case decided by the European Court of Human Rights (ECtHR), *Einarsson v Iceland*, [2017] ECHR 976 illustrates the dilemma. An Icelandic entertainment star was accused of rape and the charges against him were later dismissed. Reporting of the dismissal featured a picture of the pop star on the front page. A young man distorted the photo and posted it on Instagram with the captions "loser" and "fuck you rapist bastard". He only had 100 followers, but it was picked up by the media. The pop star sued the young man, among others, for defamation. A key question in the case was whether the statement "fuck you rapist bastard" was a factual statement or a value judgment. The Icelandic Supreme Court concluded it was a value judgment, and dismissed the defamation case, while the ECtHR disagreed, concluding that it was a statement of fact (that he was, in fact, a rapist) and therefore infringed the right to private life in article 8 of the *European Convention of Human Rights*. This illustrates how difficult it can be to assess whether content is unlawful under defamation law. If the controversial post appeared in search results, arguably this would be an inaccurate characterization of the pop star, but it depends much on the point disputed at the ECtHR, which is whether it is a statement of fact that can be inaccurate, or a value judgment beyond scrutiny of content moderators. There might be a public interest argument to continue indexing the post, but this depends on how public interest is framed. Any assessment is highly context sensitive, and this is just one post about one person.

Some of the PIPEDA factors offer an avenue for a logical, contextual analysis of the content. However, it seems unnecessary to link contextual analysis to the concept of public interest. Further, there are significant limits to a contextual analysis given the role of the private sector as "the deciders", which is explored later in this post. One avenue is to simply focus on context without shackling the freedom of expression analysis to the concept of public interest. Karen Eltis argued for a contextual analysis in defamation law, based on the civil standard, in her paper for the Law Commission of Ontario. Further, by cataloguing typical contextual issues against international human rights standards, guidance can be created—for the private sector and the OPC – for assessment of content at the margins (see, for example, Amal Clooney and Philippa Webb's guidance for assessing insulting speech against international human rights standards).

**The Role of Private Technology Companies**

I will focus here mostly on de-indexing on Google, although note the question about the role of private technology companies reaches beyond Google and search engines. As de-indexing risks becoming more mainstream, more scrutiny is needed of the system of making these decisions and the rights of the parties impacted. One option is to flag disputed content without removing it from the index, or provide a right of reply (suggested by Frank Pasquale), or flag a search query as having been amended by Google. The latter raises a privacy concern for the individual who sought de-indexing in the first place, alerting the public there is something that has been de-indexed, but recall, is still available and therefore findable online. There is no easy answer, but one clearly bad response is to open the door to one-sided de-indexing without a corresponding strengthening of the system of regulation. The OPC repairs some of these concerns with the option of making a complaint to the OPC, but that does not resolve the first responder problem.

All roads therefore lead to this system of private regulation. I have written extensively on the topic of privatization of the system of regulating human rights like free speech and privacy (see in particular here). According to the OPC, since companies already do this kind of work, such as enforcing their terms of service through various means including removing content or accounts, it is not out-of-step to impose a de-indexing obligation on search engines for privacy. Indeed, search engines de-index for a variety of situations, including for copyright infringing content. However, the fact that these companies already do this does not provide legitimacy. Indeed, the pseudo-judicial role of these companies has been the source of significant criticism over the years (see here, here, here, here and here, to name a few).

The OPC rightly points out that an expedient remedy is important for access to justice and the rule of law, which is something search engines can deliver through their own processes, at least as a first step. Indeed, the high-volume, low-value nature of many of these complaints makes formal complaints, whether to the OPC or through the courts, unfeasible to most users. We need partnerships with these companies to effectively address the kinds of harms that are facilitated through their services.

If Google is expected to play this pseudo-judicial role, consider the features of the Google courthouse. It bears little resemblance to a traditional body that balances competing rights of privacy and freedom of expression. In fact, we know very little about its system of dispute resolution, which is part of the problem.

- What are the rules?
- What is the procedure for deciding a case?
- Is there an opportunity to make submissions/be heard?
- Is there a right to hear the case against you/respond?
- Is there an appeal mechanism?
- Is the decision communicated? With reasons?
- Who is making the assessment and under what conditions? What is their training?
- Is any or all of the decision automated and what is the underlying data driving the automated system?

The reality is that despite pressure, these companies largely operate in secrecy concerning such dispute resolution processes and there are certainly no standards across industry of what such a process should look like. There are international indicia, such as the United Nations *Guiding Principles on Business and Human Rights*, which impose a duty to provide access to a forum of remediation. However, many technology companies consider their duty to respect human rights to narrowly relate to government demands that implicate privacy or free speech, not an obligation on businesses to respect the rights of users to free speech or privacy more generally (see Rikke Jørgensen) (see also Ranking Digital Rights Corporate Accountability Index). What this means is that such companies do not consider users to have a right to free speech or privacy outside what the company decides in its terms and conditions, and this too applies to their dispute resolution system. Any system of user rights and due process is driven by public pressure. I disagree with this viewpoint, but it is an unresolved debate at this point. The result is the Google courthouse resembles little the features of accountability we expect of traditionally state-run systems, such as accountability, transparency, predictability, accessibility and proportionality.

Further, the sheer quantity of content complaints has spurred two things, not just for Google, but for any major technology company grappling with illegal content. First, assessment and decision-making is increasingly automated, raising issues beyond the scope of this post (think YouTube's ContentID system). To a certain extent, some automation is critical to speedy handling of such disputes, but the implications of automation to our judicial system are a source of controversy (see, for example, this study). On a practical level, automation is not sophisticated enough to engage in a contextual analysis, which is the only avenue to balance freedom of expression and privacy (this is discussed often, but most recently, see here). Second, the quantity of content complaints has also spurred an industry of human content reviewers operating in poor working conditions and pressured to assess content within seconds (see the work of Sarah Roberts, including here). One Facebook moderator reported that she reviewed 8000 posts per day (approximately 1000 posts per hour) with a cap of one minute per post.

The OPC suggests that industry should develop a code of practice. There is merit to industry working together to provide a consistent standard for how to address these issues. It is a start, much the way that the hockey helmets are required to meet a standard that was once voluntary (Ice Hockey Helmet Regulations, SOR/2016/86). Understanding the strengths and limits of voluntary codes is key. In other work I summarized the issues of voluntary codes/corporate social responsibility (CSR) as follows:

> Pure-CSR codes simply lack the standard-setting appeal and oversight necessary to the structure of a free speech system. Such codes are too reliant on the whims or commitments of management; they are thus susceptible to change over time and unreliable as a public signal of the expectations of company conduct. A change in management, for example, can lead to a change in the business's human rights policies or, more insidiously, lead to no change in policy, but a change in the seriousness with which human rights matters are treated. The work of the Private Sector and Human Rights Project found that the commitment of particular leaders in a company was the "dominant driver for engaging with human rights". The finding was particularly the case for companies that operated outside the public sector and industry regulation,

> which would be the case for most macro-[internet information gatekeepers] such as ISPs and search engines. The problem inherent in this situation is exacerbated by the fact that IT companies, in terms of their democratic impact, are changeable, and the internet environment is unstable. This leaves the public hopelessly confused and offers none of the characteristics of due process needed to be a governance framework. Most important, it makes it more difficult to establish and sustain human rights standards. (pp 246-247)

The question for the OPC in encouraging companies to regulate through their terms and conditions is: how can industry codes be used to complement other efforts to achieve a desired objective, in this case protection of online reputation?

It is imperative that any move to enlist the help of companies comes with strong direction / expectation from government. There are various options, such as reporting requirements, through annual reports or other, mandatory dispute resolution mechanisms meeting minimum quality standards, or consideration of dispute resolution processes and other terms and conditions in assessing intermediary responsibility. In the end, the duty is on the government to protect users' privacy. The role of private parties is not that of co-regulator, but rather one element in complementary regulatory strategies to achieve privacy protection (consider education, technological design, collaboration, advocacy etc.). However, government must match the pressure it places on private companies with investment in alternative forms of dispute resolution for content-related disputes. I recommended to the LCO that online dispute resolution, specifically a tribunal, should be created for defamation disputes, and noted in the report that to be feasible, such a tribunal should be explored for a greater range of content related disputes, including privacy. This is beyond the narrow remit of the OPC, but is certainly not beyond government's attention.

**Blurring the Line Between Data Protection and Defamation Regimes**

More generally, it is unclear how this framework will operate in relation to defamation law. More work is needed to unpack this issue, but my initial thoughts wrestle with the following:

- The assessment of whether something is defamatory is different than whether something is inaccurate (the former is concerned with whether a communication lowers someone in the eyes of the community). Does this create a new avenue to resolve a reputation problem at a lower threshold?;
- The balance proposed by the OPC between freedom of expression and privacy seems to draw from defamation jurisprudence (public interest concept), but applies it differently (defamation law gives great weight to the right to free expression);
- Defamation law largely revolves around the long list of defences with the burden on the defendant to establish truth, responsibility, etc. This framework does not match the PIPEDA regime, including in particular the role of the OPC in receiving and investigating complaints. Significant work is needed to identify points of synchronicity between these regimes. Put more starkly, how *should* these regimes operate side-by-side to address online reputation issues?

- What is the relationship between privacy and defamation? There is quite a bit of scholarship on this point, and most recently see David Mangan's report to the Law Commission of Ontario. However, work here is needed as to not only the substantive nature of these rights, but how they are regulated and the access to justice issues this creates. One imagines a member of the public complaining to the OPC about online content that is outside the OPC remit but otherwise potentially unlawful.
- The obligations of intermediaries under defamation law is an issue of publication (at the moment, but see suggestions for reform). It largely operates in Canada as a notice and takedown regime. Until now, it was unclear what rights a user might have against an intermediary to remove privacy-invasive content and the proposed OPC framework would work differently. If content is potentially defamatory or inaccurate, which regime should govern?

**Conclusion**

There are many issues unexplored in this post that are critical to the OPC's position, such as the OPC's suggested geo-fencing of de-indexing, and the enforceability against American-based companies in light of section 230 of the *Communications Decency Act*, 47 USC (consider the lack of enforceability of *Google Inc. v Equustek Solutions Inc*, 2017 SCC 34 (CanLII) in *Google LLC v Equustek Solutions Inc*, 2017 (USDC N. Cali)). I sought here to focus on a few of the big issues that currently undermine the feasibility of the OPC's draft proposal.

Freedom of expression is a much more elusive concept than privacy. It can be hard to argue why it should be protected, particularly the further one is from core democratic values. However, the answer is not to tip the system in favour of privacy as starkly as the OPC has done here. Context and guidance are key and balancing these rights cannot, unfortunately, be distilled to a single concept, such as public interest, nor outsourced so easily to private parties. The OPC acknowledges the limits of its role and the need for further examination of these issues.

More generally, the OPC position paper speaks to a huge gap in Canadian law, where a major social harm meets a black hole of minimal, conflicting laws. The OPC is stretching beyond what it has the power to do in order to try to resolve some of these critical social issues. Online reputation matters and the OPC knows it, but it cannot escape its narrow remit. Teresa Scassa argues that we need to "overhaul" our data protection laws and I echo her concerns. If this report has shown anything it is that PIPEDA needs to be re-imagined in light of the digital age and broader issues of online reputation.

---

This post may be cited as: Emily Laidlaw "A Right to be Forgotten Online: A Response to the Office of the Privacy Commissioner Draft Position" (12 February, 2018), online: ABlawg, http://ablawg.ca/wp-content/uploads/2018/02/Blog_EL_OPC_Report.pdf