Stanford Law School

Center for Internet and Society
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-1417
daphnek@law.stanford.edu

Response to the Office of the Privacy Commissioner of Canada's Consultation and Call for Comments on Draft Online Reputation Position Paper

Daphne Keller
Stanford Center for Internet and Society
April 27, 2018
available at https://cyberlaw.stanford.edu/publications/comment-canadian-right-be-forgotten-proposal

Introduction

PIPEDA and similar laws are critical sources of legal protection for individuals when Internet companies collect and use information about them. They provide the correct legal framework for new, technologically enabled harms, such as the recent disclosure of Facebook user data to Cambridge Analytica. As technologies evolve, lawmakers are wise to examine existing laws like PIPEDA, to ask whether they still offer adequate protection, and to make changes if they do not.

The Office of the Privacy Commissioner of Canada (OPC) has now proposed to apply PIPEDA to a very different kind of harm: privacy violations in the form of online speech or information publicly posted by Internet users.[1] Its proposal generally tracks European Union law under the 2014 *Google Spain* ruling and subsequently enacted General Data Protection Regulation (GDPR).[2] This Comment will argue that laws developed to regulate commercial data processing, like PIPEDA, are very poorly suited for regulating online speech. It will refer to

[1] Draft OPC Position on Online Reputation, *available at* https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/#heading-0-0-4.

[2] *Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzales*, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos 2014 O.J. C 212/4 at Rul. Par. 3 http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN; Commission Regulation 2016/679, 2016 O.J. (L119) 1(EU).

these as "data protection" laws, following conventional European terminology. Data protection laws typically lack nuanced doctrines, of the sort found in other branches of privacy law or in defamation law, for balancing plaintiffs' claims against defendants' speech rights. Repurposing data protection laws as one-size-fits-all solutions for online speech harms also creates new problems, including problems of fairness in platforms' privately administered notice and takedown systems. These become particularly acute if, as suggested in the OPC's Position Paper, individuals are given data protection-based rights to eliminate online information at its source.

It is said that when the only tool is a hammer, every problem looks like a nail. This Comment submits that Canadian lawmakers have far more surgical tools for governing online speech, and do not need to rely on the hammer of data protection law. Constitutional and tort law precedent are far more doctrinally suited for weighing speech and privacy rights.[3] Internet intermediaries operating in Canada already honor content removal claims on the basis of such laws. If these long-standing bodies of law are not serving their purpose, the solution should not be to abandon them in favor of new, untested rules and far broader content removal.[4] Rather, lawmakers should consider adjusting standards and rules for their enforcement. This could include making it easier for defamation and non-data-protection privacy claimants to establish standing and recover damages. Alternately, if lawmakers conclude that PIPEDA is the proper foundation for future online speech regulation, then it should be amended to incorporate much more nuanced and stronger protections for conflicting free expression rights.

[3] *See* Law Commission of Ontario, *Defamation Law in the Internet Age*, *available at* https://www.lco-cdo.org/en/our-current-projects/defamation-law-in-the-internet-age/; *Doe 464533 v. N.D.*, 2016 ONSC 541 (identifying privacy tort claim for disclosure of embarrassing private facts).

[4] The EU's adoption of the "right to be forgotten" created what one UK practitioner called a "short cut" – a pleading or notice strategy to bypass the "lengthy debate about such terms as 'reasonable expectation of privacy', 'public domain', 'honest opinion', "'serious harm' and so on" that arose under prior law. Ashley Hurst, *Data Privacy and Intermediary Liability: Striking a Balance Between Privacy, Reputation, Innovation and Freedom of Expression, Part 1*, Inforrm's Blog (May 14, 2015), https://inforrm.wordpress.com/2015/05/14/data-privacy-and-intermediary-liability-striking-a-balance-between-privacy-reputation-innovation-and-freedom-of-expression-part-1-ashley-hurst/. Removal demands that would once have sounded (and failed) in defamation were, consequently, refiled as data protection claims.

This Comment builds on my previous, more detailed work on data protection law in the European and Inter-American legal frameworks. I do not claim expertise in Canadian law, but seek to derive lessons from other regions' experiences. Two articles are attached as appendices to the Comment. The first, *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*, is forthcoming in the Berkeley Technology Law Journal.[5] It assesses changes to the EU's "right to be forgotten" under the GDPR. Many of the issues identified in the article are directly relevant for the Position Paper's proposal. The second, *Europe's "Right to Be Forgotten" in Latin America*, reviews "right to be forgotten" proposals under the American Convention on Human Rights,[6] which protects free expression more strongly than equivalent European instruments.[7]

I come to this issue as a lawyer concerned with online speech and Internet platforms. Until 2015, I was Google's Associate General Counsel for intermediary liability. In that capacity, I worked closely with internal and external data protection experts, and gained an appreciation for the law's capabilities and complexities. Based on that experience, and on subsequent academic work at Stanford, I believe the European experience offers clear lessons for other countries considering extending data protection law as a regulatory framework for online speech.[8] Without substantial modification, data protection law will not provide adequate doctrinal tools for balancing privacy and free expression interests.

---

[5] Keller 2018, *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2914684.

[6] Canada is not a signatory to the Convention, but protects free expression rights strongly under its own human rights and constitutional framework.

[7] Keller 2017, *available at* http://cyberlaw.stanford.edu/publications/europes-right-be-forgotten-latin-america-0 in English and http://cyberlaw.stanford.edu/publications/el-derecho-al-olvido-de-europa-en-america-latina-0 in Spanish. A more detailed student-authored review of human rights sources and case law developments, *The "Right to Be Forgotten" and Blocking Orders under the American Convention: Emerging Issues in Intermediary Liability and Human Rights* (2017), is at https://law.stanford.edu/publications/the-right-to-be-forgotten-and-blocking-orders-under-the-american-convention-emerging-issues-in-intermediary-liability-and-human-rights/.

[8] The Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School. A list of CIS donors and funding policies is available at https://cyberlaw.stanford.edu/about-us.

Sources of Law for Balancing Rights

For intermediaries like Google or Facebook, data protection laws may govern the use of two very different types of data. The first is data that platforms collect about individual Internet users – such as their clicks, browsing behavior, or account information. If Bob is a Facebook user and wants to delete his account or control how his data is shared, data protection law can provide the legal right to do so. Application of laws like PIPEDA to this privately held, back-end data is relatively straightforward. Strengthening PIPEDA or other data protection laws to address emergent problems involving this kind of data is reasonable and appropriate.

The second kind of data is expressive content shared online by individual Internet users. If Alice posts a Facebook comment about Bob, does Bob have a right to make Facebook delete it? This question raises difficult constitutional issues of the sort historically unaddressed by data protection. An organization or lawmaker assessing Bob's claim must consider the conflicting rights of multiple individuals – including Alice and any Internet users with a legitimate interest in the information she posted. Data protection rules derived from the simpler two-party situation (individual privacy claimant versus business) are mismatched to this more complex task.

The question here is not whether data protection law *can* be interpreted to cover expressive content put online by users, but whether it *should* be. Clearly such interpretations are possible – the CJEU demonstrated that in *Google Spain*. Equally clearly, the CJEU's interpretation was not mandatory or inevitable. The court's own Advocate General had urged the opposite outcome.[9] The letter of data protection law, under both the EU's Data Protection Directive and PIPEDA, can be read both ways.

[9] The Advocate General concluded that Google in most cases does not act as a controller, and that EU data protection law did not create a right to "be forgotten" by deleting publically available information based on the data subject's personal preference. Opinion of Advocate General Jääskinen, Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ¶¶89, 111. *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN. (May 13, 2013). The

Equally, the question is not *whether* individuals injured by online disclosure of personal or false information should have any remedy, or any mechanism to make Internet intermediaries take the content down. In both the EU and Canada, these rights exist. The question is *how* these rights should be defined and enforced. Data protection law is not the only option. As former Yale Law School Dean Robert Post has written, the *Google Spain* court had a choice between two bodies of law on which to base a "right to be forgotten."[10] The first body of law, grounded in Article 7 of the EU Charter, includes traditional tort claims addressing dignitary and reputational harms, such as defamation or invasion of privacy. These long-established claims "define and enforce social norms of respectful expression"[11] and are designed to uphold "public communications governed by norms of propriety in which information is the medium of an intersubjective dialogue[.]"[12] The second body of law, grounded in Article 8 of the EU Charter, is data protection. Data protection is newer. It provides more mechanistic rules, designed to "define and enforce the proper bureaucratic handling of data."[13] Post argues that the CJEU erred – and missed an opportunity to provide better precedential guidance – in conflating the two.

CJEU most often follows the advice of the Advocate General, but did not in this case. *See generally* Carlos Arebola et al., *An Econometric Analysis of the Influence of the Advocate General on the Court of Justice of the European Union*, 5 Cambridge J. Comp. Int'l L. 1, (2016).

[10] *Data Privacy and Dignitary Privacy: Google Spain, the Right to Be Forgotten, and the Construction of the Public Sphere*, 67 Duke Law Journal 981 (2018), *available at* ssrn.com/abstract=2953468. Post refers to the "distinct bureaucratic version of the right to be forgotten" under data protection law as "RTBF," and uses the term "right to be forgotten" to refer to "the more traditional version of the right that protects dignitary privacy[.]" As he explains,

> The RTBF imagines a bureaucratic world that conforms to an instrumental logic in which data are gathered and used for "specified purposes." The right to be forgotten, by contrast, presupposes a world of public communications… The RTBF applies to data management; the right to be forgotten applies to communication. The object of the RTBF is to give data subjects "control" over their personal data; the object of the right to be forgotten is to protect the dignity of human beings. Although the RTBF makes sense in the context of large organizations that assemble big data to accomplish explicit purposes, its managerial logic is fundamentally incompatible with the communicative action required by the democratic public sphere. The right to be forgotten, by contrast, has been applied to the democratic public sphere in most legal systems for more than a century. *Id.* at 993-994 (internal citations omitted).

[11] *Id.* at 992.

[12] *Id.* at 993.

[13] *Id.* at 991-2.

Data protection law does have some advantages as a legal tool for responding to the spread of harmful online information. Unlike defamation or traditional privacy law, it is designed to regulate automated, high-volume data processing. It also comes pre-equipped with regulatory enforcement bodies such as the OPC. Data protection law's disadvantage, though, is serious. It has not evolved through generations of litigation, legislation, and scholarship to balance complex individual rights claims, particularly those relating to speech. Shifting laws about individual speech rights to a data protection framework effectively cuts them off from their legal history, and strips speakers, intermediaries, and claimants of longstanding guidance about free expression rights and acceptable speech.

Applying data protection law to online speech also creates new doctrinal headaches and unintended consequences. Under European data protection law, for example, businesses acting as data controllers must seek consent before processing information about an individual's health or other sensitive topics. Enforcing this rule for online speech processed by intermediaries leads to absurd results.[14] It puts search engines in violation of law from the moment they index online gossip about a celebrity's pregnancy, for example -- or puts Facebook in violation every time a user posts a get-well note to a friend. As one prominent European scholar wrote, applying the plain language of the Data Protection DIrective would make search engines literally "incompatible with EU law," because they are "unable to comply with most of the obligations the Directive imposes on data controllers."[15] The Position Paper's discussion of search engines and consent suggests that a similarly fundamental problem may exist under PIPEDA.

[14] This problem in applying data protection law to itermediares will be addressed in a pending CJEU case. *See* Conseil d'Etat, *Right to Be Delisted*, (February 24, 2017) http://english.conseil-etat.fr/Activities/Press-releases/Right-to-be-delisted.

[15] Miquel Peguera, *The Shaky Ground of the Right to be Delisted*, 18 Vand. J. of Ent. & Tech. L. 507, 539.

This is by no means the only doctrinal glitch that arises when data protection law is used as a one-size-fits-all regulatory tool for both back-end data and online speech. The attached article identifies numerous examples of similar problems under the GDPR. For example, a data subject may compel a controller to disclose "any available information" about the source from which it obtained her personal data.[16] When the source of information is an individual Internet user who posted speech online, and who herself relies on the platform to keep her account information confidential, disclosing her information makes no sense and runs counter to the GDPR's purposes. Yet the GDPR identifies no exceptions for this situation, presumably because drafters were thinking of the simpler situation in which one business passes data to another.

As another example, a data subject who alleges that information is inaccurate may, under the GDPR, instruct the controller to immediately restrict it from public access.[17] This restriction takes place before the controller even assesses any objection to processing or "right to be forgotten" erasure request. This default in favor of immediate data restriction may make sense in contexts such as commercial ad targeting or profiling. As a rule for restraint of online speech, though, it is dangerous.

Unintended consequences such as these generally arise in the Alice/Bob situation -- when one individual seeks to limit access to another's speech. In rare but important cases, though, the public interest is disserved by allowing an individual to delete her *own* speech. The OPC says that the right to do so should "be near-absolute, except to the extent that it is subject to legal or contractual restrictions," which presumably is correct as a matter of PIPEDA interpretation. The lack of a further public interest exception to this rule, however, illustrates the hazards in extending data protection law to public

[16] GDPR Art. 14(2)(f), 15(1)(g). *See The Right Tools* Section III.C.4.b (Giving the Requester Personal Information About the Speaker); *See also* GDPR Art. 17(2); 19 (requiring controller to share information about erasure requests with third parties); *The Right Tools* Section III.C.4.a (Telling Controllers and the Requester).

[17] GDPR Art. 18. It is very hard to parse the application of this requirement to online content removal. It appears to require platforms to assess the same speech twice, under slightly different standards. *See The Right Tools* Section III.C.2 (Temporarily "Restricting" Content).

speech. Consider US President Donald Trump's Twitter posts, which are often the sole source of key policy announcements, as well as important evidence of his inconsistencies over time. The OPC suggests that PIPEDA would give President Trump – or any business leader, politician, or individual pruning her public history before announcing a political candidacy -- a right to delete this public record.

Procedures for Taking Down Online Speech

Extending PIPEDA to online content would effectively create two new processes for deciding which speech is de-listed or removed. One would be privately administered by Internet companies, the second by regulators and courts. Both would follow procedural rules that tilt the playing field against speech rights online, and in favor of content removal.[18]

Platform-administered notice and takedown systems of the sort proposed in the Position Paper are common around the world. They bring important benefits, by allowing speedy relief for people harmed by online information. But they also impose well-documented costs on other Internet users. Claimants routinely abuse the systems, sending platforms legally baseless notices as a means to silence other people's lawful expression. Governments suppressing criticism, religious organizations stifling dissent, and disgraced professionals seeking to hide their past misdeeds have all used bogus notices in this manner.[19] A 2006 study of notices submitted to Google web search found that more than half came from competitors targeting one another's

[18] The equivalent issue under the GDPR is addressed in detail in *The Right Tools* Section III.C (Notice-and-Takedown Process).

[19] José Miguel Vivanco, *Censorship in Ecuador has made it to the Internet* (2014), originally published in *El Pais*, *available at* https://www.hrw.org/news/2014/12/15/censorship-ecuador-has-made-it-internet; Eva Galperin, *Massive Takedown of Anti-Scientology Videos on YouTube*, ELECTRONIC FRONTIER FOUND. (September 5, 2008), https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube; John Timmer, *Site plagiarizes blog posts, then files DMCA takedown on originals*, ARS TECHNICA (February 5, 2013, 3:33 PM), http://arstechnica.com/science/2013/02/site-plagiarizes-blog-posts-then-files-dmca-takedown-on-originals/.

businesses, and 31% raised dubious legal claims.[20] Under the EU's "right to be forgotten" laws, both Microsoft and Google say over 50% of requests they receive are legally invalid.[21]

Intermediaries far too frequently comply with abusive or mistaken notices. This is to be expected: taking content down is nearly costless, leaving it up creates litigation risk and requires paying lawyers to assess claims. The major empirical work in the field reported that some of the studied businesses simply honored *every* request they receive, and most opted "to take down content even when they [were] uncertain about the strength of the underlying claim."[22]

Major platforms like Google or Facebook employ thousands of moderators and build sophisticated content management tools, but nonetheless often take down the wrong things – as when YouTube recently removed human rights' organizations videos documenting Syrian war crimes.[23] Civil rights organizations charge that platforms are particularly prone to remove lawful speech of minority or socially marginalized speakers.[24] Notice-and-takedown systems come with a real cost to lawful public participation.

---

[20] Jennifer Urban and Laura Quilter, *Efficient Process or 'Chilling Effects'? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 SANTA CLARA COMP. HIGH TECH. L. J., 621, 651 & 667 (2005). *See also* Rishabh Dara, *Intermediary Liability in India: Chilling Effects on Free Expression on the Internet 2011*, CTR. FOR INTERNET & SOC'Y, http://cis-india.org/internet-governance/intermediary-liability-in-india.pdf (last visited September 19, 2017); Christian Ahlert, et al., *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation*, CTR. FOR SOCIO-LEGAL STUD.: PROG. IN COMP. MEDIA L. & POL'Y, http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf (last visited September 19, 2017); John Leyden, *How to Kill a Website with One Email: Exploiting the European E-Commerce Directive*, THE REGISTER, (October 14, 2004), http://www.theregister.co.uk/2004/10/14/isp_takedown_study/.

[21] Google Transparency Report, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/; Microsoft Content Removal Requests Report, MICROSOFT, https://www.microsoft.com/about/csr/transparencyhub/crrr/. Data Protection Authorities reviewing de-listing claims rejected by the companies concluded that "in the great majority of cases the refusal by a search engine to accede to the request is justified." This suggests that the self-reported 50% rate of improper requests is roughly accurate by regulators' standards. *Article 29 Data Protection Working Party, Press Release* (June 18, 2015) http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20150618_wp29_press_release_on_delisting.pdf.

[22] See Jennifer M. Urban et al., *Notice and Takedown in Everyday Practice* at 41, (March 29, 2016) UC Berkeley Public Law Research Paper No. 2755628 (2016) at 41, https://ssrn.com/abstract=2755628.

[23] Malachy Browne, "YouTube Removes Videos Showing Atrocities in Syria," The New York Times, August 22, 2017; Scott Edwards, "When YouTube Removes Violent Videos, It Impedes Justice," Wired, October 7, 2017.

[24] Sam Levin, "Civil rights groups urge Facebook to fix 'racially biased' moderation system," The Guardian, January 18, 2017; Tracy Jan and Elizabeth Dwoskin, "A white man called her kids the n-word. Facebook stopped her from sharing it," The Washington Post, July 31, 2017.

To better protect Internet users' expression rights, numerous civil society organizations have demanded improvements to notice and takedown procedures.[25] Widely endorsed protections for online speech include notice to the speaker and opportunity to object; penalties for bad faith removal demands; and opportunities for appeal and judicial review. Human rights leaders within the UN and Organization of American States have called for similar measures.[26]

The de-listing process proposed in the Position Paper would move in the other direction, further weakening protections for online speakers within platforms' privately administered notice and takedown systems. Most troublingly, it would follow Europe's model in limiting notice to webmasters whose pages are de-listed. This prohibition creates substantial imbalance between the rights of the accuser and those of the accused. In Mexico, an appellate court reviewing a "right to be forgotten" case found this imbalance constitutionally inadequate, and held that online publishers must be given notice and the opportunity to defend themselves.[27]

The procedural advantage enjoyed by claimants in platforms' private notice and takedown systems would, following the Position Paper, be replicated in OPC and court review processes. Privacy claimants would have recourse to administrative review by the OPC if an intermediary failed to honor a removal request. People whose speech was wrongly de-listed or removed would not. Nor would the law provide them with any equivalent procedural recourse or source

[25] Manila Principles on Intermediary Liability, *available at* manilaprinciples.org.

[26] *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN (2016), *available at* https://perma.cc/44AY-ZX9G (Manila Principles "establish baseline protection for intermediaries in accordance with freedom of expression standards"); *Standards for a Free, Open and Inclusive Internet* (2017), OAS Office of the Special Rapporteur for Freedom of Expression (platform notice and takedown systems "do not always respect the right to due process and minimum guarantees, insofar as they shift the responsibility to examine and decide on the lawfulness or unlawfulness of the content," and are compatible with the American Convention on Human Rights only "to the extent that they establish sufficient safeguards for the protection of the users' freedom of expression and due process, and do not impose vague or disproportionate obligations on intermediaries").

[27] *La Fortuna v. INAI, Expediente Auxiliar*, 355/2016, *available at* https://perma.cc/5WQC-JJMV.

of government support.[28] The resulting imbalance would affect both individuals asserting constitutional rights and the development of important legal precedent. The OPC and courts would have opportunity to review and correct platforms only when they removed too *little* speech – never when they removed too *much.*

Federalism Concerns

The Position Paper also raises important questions about provincial and federal power. These have some analog in the European implementation of the GDPR, but appear to be more pronounced in the Canadian context.

As a 2018 House of Commons Committee report explains, "reputational damage that occurs within the framework of personal relationships rather than commercial transactions does not fall under PIPEDA, but generally under provincial legislation governing tort and civil liability."[29] Personal relationships, however, are often conducted over commercial Internet platforms. For people under a certain age, it would be highly unusual for relationships *not* to involve text messages, Facebook and WhatsApp posts,

[28] Online speakers may have actionable constitutional claims in this situation regardless of whether they have a legal "right" to be hosted or indexed by a private platform in the first place. Speakers' constitutional rights are engaged when state action, in the form of a legal mandate, causes a private actor to erase or de-list their speech. See, e.g., *Magyar Tartalomszolgáltatók Egyesülete (MTE) v. Hungary (2016)* E.Ct.H.R. 82, http://www.bailii.org/eu/cases/ECHR/2016/135.html (state violated Internet users' free expression rights under European Convention by imposing strict liability and de facto monitoring obligation on hosting platform); *Smith v. California*, 361 U.S. 147 (1959); (state violated U.S. readers' and publishers' First Amendment rights by imposing strict liability on bookseller); *Bantam Books, Inc. v. Sullivan* 372 U.S. 58 (1963) (state violated First Amendment by administrative order liability on bookseller); Christina Angelopoulos et al, *Study of fundamental rights limitations for online enforcement through self-regulation*, 50-51 (2016), IVIR, http://www.ivir.nl/publicaties/download/1796 (EU Member States may violate human rights law by mandating or supporting overbroad removal by platforms); Aleksandra Kuczerawy, The Power of Positive Thinking: Intermediary Liability and the Effective Enjoyment of the Right to Freedom of Expression, *forthcoming in: JIPITEC 'Intermediary Liability as a Human Rights Issue' (2017)* (European human-rights-based limits on intermediary liability laws including notice and takedown procedures).

[29] *Towards Privacy By Design: Review of The Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics, House of Commons, Canada (2018) at 36, *available at* http://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf Even for questions properly answered by data protection law, provincial equivalents of PIPEDA may in some cases take priority over the federal legislation. *Id*. at 13.

or similar platform-based communications. Regulating content on a platform like Twitter or Facebook unavoidably affects these personal relationships. The OPC's interpretation of PIPEDA effectively moves governance of reputational damage in this sphere from provincial hands to federal ones.[30]

A similar issue arises in the EU, where Member States hold authority over free expression protections. Under both the GDPR and the 1995 Data Protection Directive, Member States are charged with reconciling privacy and free expression in their national law.[31] As Cambridge University's David Erdos has documented, different countries have struck very different balances between privacy and free expression rights.[32] As a result, a de-listing request that might be valid in Poland, for example, might be properly rejected on free expression grounds in Denmark. This diversity of national outcomes is not a bug, but a feature arising from the allocation of authority between central and state government. It creates complications, however, for Internet intermediaries implementing de-listing or removal requests. Should Poland's rules constrain information access in Denmark? Should platforms implement state-by-state geoblocking for content that is legal in one region but not the other?[33] This question, too, is raised in a pending CJEU case.[34]

The Position Paper would seem to avoid these issues by adopting a single federal framework to govern reputational damage online. Canada's federal system and reservation of powers to provinces may, however, complicate this approach.

[30] It is unclear when claimants would rely on province-level tort claims, since data protection claims appear to be both procedurally simpler and likelier to succeed.
[31] GDPR Art. 85.
[32] Erdos has published extensively on the topic, most recently in *Beyond 'Having a Domestic'? Regulatory Interpretation of European Data Protection Law and Individual Publication* (2016), University of Cambridge Faculty of Law Research Paper No. 54/2016, *available at* https://ssrn.com/abstract=2847628.
[33] As discussed in *The Right Tools*, the practical consequence may simply be that the more speech-restrictive rule is enforced broadly. See Section III.E.2 (Territorial Scope of Compliance: Must OSPs Erase Content Globally?).
[34] *Google Inc.*, Case No. 399922 (July 19, 2017), Conseil d'Etat, France, http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC.

Removing Content at the Source?

The Position Paper indicates that PIPEDA provides rights, not only to de-index information in web search results, but to take down information "at the source." This proposal appears to go well beyond any clear rule of the CJEU or GDPR, although the application of "right to be forgotten" claims to hosts or other online sources is evolving.[35] The implications of removing data from online sources vary depending on which sources are affected.[36]

First, does the proposal apply directly to online publishers, such as the operator of a personal webpage about gardening, poetry, sports, or history? Presumably the answer turns in part on commerciality. Does such a site become "commercial" enough to fall under PIPEDA if it relies on advertisements, subscriptions, or online tip jars for support? Can some or all publishers claim exemptions based on "journalistic, artistic, or literary" use of information?

If "sources" regulated under PIPEDA are not publishers themselves, but only commercial hosts of third party content, other questions arise. Many publishers depend on web hosts like Amazon Web Services as infrastructure providers. Can individuals bring removal demands directly to these technical hosting services, and bypass the publisher? That would take a publisher's ability to control and defend her own speech out of her hands – unless she assumed the expense and complexity of running her own server. Is the legal answer different if a publisher uses a more end-user-oriented platform, such as Medium or Facebook?

[35] See *The Right Tools* Section III.B (Right to Be Forgotten Obligations for Hosts and Social Media); Case N° C.15.0052.F, Belgian Cour de Cassation, April 29, 2016 (ordering news archives to redact stories), *available at* https://inforrm.files.wordpress.com/2016/07/ph-v-og.pdf; *C.F. v. Primadanoi* 13161/16, Italian S. Ct, April 11, 2015 (holding that newspaper's expression rights in a two-year-old news report had expired "just like milk, yoghurt or a pint of ice-cream" and requiring deletion of identifying information), *discussed in* Athalie Matthews, How Italian courts used the right to be forgotten to put an expiry date on news, The Guardian (September 20, 2016), https://www.theguardian.com/media/2016/sep/20/how-italian-courts-used-the-right-to-be-forgotten-to-put-an-expiry-date-on-news.

[36] This high-level overview draws on non-Canadian law. These questions may play out differently in the EU because of legal mechanisms like the controller/processor distinction, household use exception, and new broader free expression provisions in Article 85 of the GDPR.

How about consumer review sites like Yelp? Can waiters, mechanics, doctors, and accountants now remove negative reviews based on PIPEDA? Are consumer reviews protected as journalistic works? Does the answer depend on Yelp's judgment about what criticisms are professionally relevant (slowness, rudeness, bad breath) as well as which factual claims are accurate?

Does a hosting service's legal obligation vary depending on its size and capabilities? The Position Paper states that users should be able to delete social media posts "independently, without having to make a request subject to the organization's response." Facebook or YouTube certainly have the means to provide such deletion tools. Many more modest businesses and websites that allow users to post comments, however, do not. Must they stop permitting user comments? Similar questions arise with respect to small platforms' investment in geoblocking technologies for regionalized legal compliance.

Conclusion

PIPEDA and data protection law are not good legal tools for regulating online speech. They lack well-developed standards to balance and protect expression rights, and they introduce unintended consequences that may do damage to both speech and privacy rights. Existing law from areas like defamation, and existing legal and civil society frameworks for intermediary liability, provide a far better way forward in addressing reputational harms online.