Osgoode Hall Law Journal

Volume 55, Issue 2 (Spring 2018) Article 1

9-4-2018

Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow

Andrea Slane
University of Ontario Institute of Technology

Citation Information

Slane, Andrea. "Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow." *Osgoode Hall Law Journal* 55.2 (2018) : 349-397.
DOI: https://doi.org/10.60082/2817-5069.3288
https://digitalcommons.osgoode.yorku.ca/ohlj/vol55/iss2/1

Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow

Abstract

The Office of the Privacy Commissioner of Canada ("OPC") recently proposed that Canada's private sector privacy legislation should apply in modified form to search engines. The European Union ("EU") has required search engines to comply with its private sector data protection regime since the much-debated case regarding Google Spain in 2014. The EU and Canadian data protection authorities characterize search engines as commercial business ventures that collect, process, and package information, regardless of the public nature of their sources. Yet both also acknowledge that search engines serve important public interests by facilitating users' search for relevant information. This article considers specifically what a Canadian right to be forgotten might look like when it is seen as an opportunity to re-balance the values at stake in information flow. This article aims to bring Canada's existing legacy of balancing important values and interests regarding privacy and access to information to bear on our current information environment.

Keywords

Right to be forgotten; Search engines--Law and legislation; Canada

Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow

ANDREA SLANE*

The Office of the Privacy Commissioner of Canada ("OPC") recently proposed that Canada's private sector privacy legislation should apply in modified form to search engines. The European Union ("EU") has required search engines to comply with its private sector data protection regime since the much-debated case regarding Google Spain in 2014. The EU and Canadian data protection authorities characterize search engines as commercial business ventures that collect, process, and package information, regardless of the public nature of their sources. Yet both also acknowledge that search engines serve important public interests by facilitating users' search for relevant information. This article considers specifically what a Canadian right to be forgotten might look like when it is seen as an opportunity to re-balance the values at stake in information flow. This article aims to bring Canada's existing legacy of balancing important values and interests regarding privacy and access to information to bear on our current information environment.

* Associate Professor in the Legal Studies Program at the University of Ontario Institute of Technology.

AS EVIDENCED BY COMMON SLOGANS like 'lest we forget' and let 'bygones be bygones,' 'remembering' and 'forgetting' play important social functions: We need to both learn from history and be able to move on from the past. The right to be forgotten that has entered global public consciousness in the last few years has inspired both concerns about suppressing history[1] and reminders that total remembering is both new and damaging to data subjects and communities.[2] However, the impetus behind the right to be forgotten is less about grand social values of remembering and forgetting, and more about managing personal information flows in the digital age: It is about trying to address vast power imbalances between data subjects and various digital information brokers, including information location service providers such as search engines.[3]

In Canada, the Office of the Privacy Commissioner of Canada ("OPC") recently proposed that the data protection regime governing the private sector, the *Personal Information Protection and Electronic Documents Act* ("*PIPEDA*"), should be interpreted to obligate search engines to abide by fair information principles, in particular the principles of accuracy and appropriate purposes.[4] Applying *PIPEDA* to search engines would be a new practice, even though the

1. Pierre Trudel, "La menace du « droit à l'oubli »" (11 April 2014), *Blogues Pierre Truedel* (blog), online: <www.journaldemontreal.com/2014/04/11/la-menace-du--droit-a-loubli>.
2. Viktor Mayer-Schönberger, *Delete: The Virtue of Forgetting in the Digital Age* (Princeton, NJ: Princeton University Press, 2011); Napoleon Xanthoulis, "The Right to Oblivion in the Information Age: A Human-Rights Based Approach" (2013) 10:1 US-China L Rev 84 at 96-97.
3. Julia Powles, "The Case That Won't Be Forgotten" (2015) 47:2 Loy U Chicago LJ 583 at 586.
4. SC 2000, c 5 [*PIPEDA*]; Office of the Privacy Commissioner of Canada, *Draft OPC Position on Online Reputation* (Gatineau, Que: Office of the Privacy Commissioner of Canada, 2018), online: <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801> [OPC, *Draft OPC Position*].

OPC claims that it is merely applying the current legislation. As recently as 2017, it seemed that only voluntary cooperation would be requested of search engines. For example, in the Federal Court's affirmation of the OPC findings in *AT v Globe24h.com*, the defendant's website was found to have violated *PIPEDA* when it scraped court and tribunal documents containing personal information from publicly accessible legal databases and allowed them to be indexed by general search engines.[5] The Federal Court issued a declaratory court order, as endorsed by the OPC, which allowed the complainant to appeal to Google to honour its voluntary search alteration policies: The court did not directly issue an order to compel Google to do so.[6]

The European Union ("EU"), however, already requires search engines to honour complainants' requests to remove personal information from search results in certain circumstances. The data protection regime in the EU characterizes search engines as primarily commercial business ventures that collect, process, and package information, regardless of the public nature of their sources.[7] Search engine results are in this sense a product sold by the search engine company—not directly to the user, but rather to advertisers and other data brokers with an interest in search result content and compilation. If this understanding of search engine results as an information product were adopted in Canada, as currently proposed by the OPC, then a search engine company could be deemed to be subject to *PIPEDA*, in that it "collects, uses or discloses [personal information] in the course of commercial activities."[8] While the OPC has rightly suggested that it would be unreasonable to require search engines to abide by *PIPEDA* as a whole, in particular with regard to securing consent for all of its collection and use of

5. *AT v Globe24h.com*, 2017 FC 114 at para 101, 407 DLR (4th) 733 [*Globe24h*]. See also *Regulations Specifying Publicly Available Information*, SOR/2001-7 [*RSPAI*] (demonstrating that much of the reasoning in *Globe24h* involves interpretation of the *RSPAI*).
6. *Globe24h*, *supra* note 5 at para 86. See also *AT v Globe24h.com*, 2017 FCC 114 (Memorandum from Privacy Commissioner of Canada, the Added Respondent, Added Respondent's Record, Vol 4, Tab 6 at 1016-49, Federal Court File No T-1248-15).
7. European Commissioner, Viviane Reding, considers the right to be forgotten as merely strengthening existing obligations under European data protection law. See Bert-Jaap Koops, "Forgetting Footprints, Shunning Shadows. A Critical Analysis of the 'Right to be Forgotten' in Big Data Practice" (2011) 8:3 SCRIPTed 229 at 232-33, 244.
8. *PIPEDA*, *supra* note 4, s 4; OPC*, Draft OPC Position, supra* note 4.

personal information,[9] there are nonetheless significant ways that *PIPEDA* could be applied in a workable and rights-balancing way. This article considers what a finding that search engines are subject to *PIPEDA* would mean, and how it could be justified and limited in a principled fashion that respects our commitment to privacy, access to information and freedom of expression. In other words, what would a Canadian right to be forgotten look like?

The right to be forgotten is generally recognized as arising from European sensibilities regarding personality rights.[10] European privacy and identity rights provide strong protections for individual autonomy in the domain of identity formation and presentation, giving individuals more control over how they are discussed and portrayed in public. European data protection law operates as an outgrowth of this broader and stronger protection of citizens' identity. This commitment is rooted in European emphasis on human dignity, respect for one's 'private life,' and protection from damage to one's reputation by either government or private actors.[11] These rights are enshrined in multiple constitutional documents of the EU,[12] and illustrate the more general trust that

9. OPC, *Draft OPC Position*, *supra* note 4; Office of the Privacy Commissioner of Canada, *Real Fears, Real Solutions: A plan for restoring confidence in Canada's privacy regime*, 2016-17 Annual Report to Parliament on the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act* (Gatineau, Que: Office of the Privacy Commissioner of Canada, 2017), online: <www.priv.gc.ca/media/4586/opc-ar-2016-2017_eng-final.pdf> [*OPC Consent Report*].
10. Ignacio Cofone, "Google v. Spain: A Right To Be Forgotten?" (2015) 15:1 Chi-Kent J Intl & Comp L 1 at 2; Meg Leta Ambrose, "It's About Time: Privacy, Information Life Cycles, and the Right to be Forgotten" (2013) 16:2 Stan Tech L Rev 369 at 380-81; Aidan Forde, "Implications of the Right to be Forgotten" (2015) 18:1 Tul J Tech & Intell Prop 83 at 85.
11. Ambrose, *supra* note 10 at 374; Meg Leta Ambrose & Jef Ausloos, "The Right to be Forgotten Across the Pond" (2013) 3 J Info Pol'y 1 at 14; Rolf H Weber, "The Right To Be Forgotten: More Than a Pandora's Box?" (2011) 2:2 J Intell Prop Info Tech & E-Commerce L 120.
12. EC, *Charter of Fundamental Rights of the European Union*, [2012] OJ, C 326/02, arts 7-8; Council of Europe, *Convention for the Protection of Human Rights and Fundamental Freedoms*, European Treaty Series No 005, art 8 (entered into force 4 November 1950), online: <https://www.echr.coe.int/Documents/Convention_ENG.pdf>.

European legal culture places in government regulation to protect these interests, and their distrust of private markets to do so.[13]

The United States, on the other hand, is often regarded as having the opposite of European sensibilities when it comes to personal information flow. In the United States, privacy is rooted in liberty rather than dignity, as a right to be 'free from' government interference in one's private life, with far fewer and more limited restrictions placed on private actors.[14] Constitutional protection for privacy only extends to unreasonable search and seizure, and any private rights to privacy are consequently derived from statute or common law and often lose out to the much stronger constitutional protection for freedom of speech, which is notoriously strong in the United States.[15] US legal culture stresses an acute distrust of government regulation, and instead places much more trust in markets to deal with private problems.[16]

Canada tends to fall somewhere in between these two interpretations: Our *Charter of Rights and Freedoms* does not contain express protection for privacy beyond protection from unreasonable search and seizure—although Quebec's additional *Charter of human rights and freedoms* does, and is closer to the European approach to privacy, using similar language in fostering respect for "private life."[17] However, section 1 of the Canadian *Charter* has allowed privacy interests to be more readily balanced against freedom of expression than in the United States, as more restrictions can be justified as reasonable in a "free and democratic

---

13. Franz Werro, "The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash" in Aurelia Colombi Ciacchi et al, eds, *Haftungsrecht im dritten Millennium - Liability in the Third Millennium* (Baden-Baden: Nomos, 2009) 287 at 299; Éloïse Gratton & Jules Polonetsky, *Privacy above all other Fundamental Rights? Challenges with the Implementation of a Right to be Forgotten in Canada* (Gatineau, Que: Office of the Privacy Commissioner of Canada, April 2016) at 2, online: <www.eloisegratton.com/files/sites/4/2016/04/PolonetskyGratton_RTBFpaper_FINAL.pdf>. This report was submitted by Éloïse Gratton & Jules Polonetsky to the Office of the Privacy Commissioner of Canada as part of its consultation and call for essays on online reputation. See "Consultation on online reputation," Office of the Privacy Commission of Canada, online <www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation>.
14. James Q Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty" (2004) 113:6 Yale LJ 1151 at 1214.
15. Ambrose, *supra* note 10 at 375.
16. Gratton & Polonetsky, *supra* note 13 at 2.
17. *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*]; *Charter of human rights and freedoms*, CQLR c C-12, s 5; arts 3, 35-36 CCQ. For discussion of the differences between Quebec and the rest of Canada regarding privacy and personality rights, see Gratton & Polonetsky, *supra* note 13.

society."[18] Canada consequently approaches some issues of personal information flow differently than the United States—for example, publication bans to protect the privacy of some crime victims are constitutionally possible in Canada but not in the US.[19] However, Canada has not embraced personality rights to the extent that the EU has, and significant recent gains in Canada for freedom of expression (specifically regarding publication of defamatory content) illustrate that Canada places more value on freedom of expression and less on protecting reputation than Europe.[20] Canadian law on intermediary liability for information posted online by others is also less developed than in these jurisdictions.[21]

Discussions about the right to be forgotten are emerging along with the rapid development of our technology-based information landscape.[22] Real concerns about actual and potential pervasive surveillance—from government, companies, peers, and the broader public—have resulted in heightened anxiety about being able to protect one's identity and interests.[23] Revelations of broad government surveillance of communications, commercial entities amassing vast quantities of data about consumer behaviour (including emotional responses to various stimuli, tracking online and app-enabled interactions with others, and geo-location technologies in many portable devices), as well as the explosion of social media, have fueled these concerns.[24] Anonymity has always been a central strategy for protecting one's privacy online,[25] but it is becoming increasingly difficult to remain unidentified.[26] We all now have large dossiers with data held by various

---

18. *Charter*, *supra* note 17, s 1.
19. *Canadian Newspapers Co v Canada (Attorney General)*, [1988] 2 SCR 122, 52 DLR (4th) 690.
20. Iris Fischer & Adam Lazier, "*Crookes v. Newton*: The Supreme Court of Canada Brings Libel Law into the Internet Age" (2012) 50:1 Alta L Rev 205 at 217; Karen Eltis, "Can the Reasonable Person Still be 'Highly Offended'? An Invitation to Consider the Civil Law Tradition's Personality Rights–Based Approach to Tort Privacy" (2008) 5:1&2 UOLTJ 199.
21. Corey Omer, "Intermediary Liability for Harmful Speech: Lessons from Abroad" (2014) 28:1 Harv JL & Tech 289 at 305.
22. Mayer-Schönberger, *supra* note 2.
23. Meg Leta Jones, *Ctrl+Z: The Right to Be Forgotten* (New York: New York University Press, 2016).
24. Colin J Bennett et al, *Transparent Lives: Surveillance in Canada* (Edmonton: Athabasca University Press, 2014).
25. Chris Hunt & Micah Rankin, "*R. v. Spencer*: Anonymity, the Rule of Law, and the Shrivelling of the Biographical Core" (2015) 61:1 McGill LJ 193; Carole Lucock & Michael Yeo, "Naming Names: The Pseudonym in the Name of the Law" (2006) 3:1 UOLTJ 53.
26. Paul Ohm, "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization" (2010) 57:6 UCLA L Rev 1701 at 1716-22; Bennett et al, *supra* note 24 at 19.

public, private, and personal actors, with little knowledge of what is in them, and how they are combined (including from both private and public sources). Proponents of the right to be forgotten are attempting to intervene against this power imbalance.[27]

Search engines have become the primary means by which we find information, including of course about people: We search for people we know or hear about, and occasionally check our own names.[28] Google has emerged as the worldwide leader in online search services, credited with over 90 per cent of the global market share.[29] Google's success has been attributed to its algorithms, by which the company processes information gathered from publicly available webpages and delivers the results in list form to a user, partly based on the user's previous search history.[30] The aim is to deliver the most relevant material at the top of the list. Information presented further down the list is deemed less relevant and most people do not even look at search results beyond the first page or two.[31] Online reputation management services have long profited from the willingness of companies and individuals to pay for techniques such as Search Engine Optimization ("SEO") to manipulate search results so positive information rises to the top and negative information is pushed down the list.[32] These services are expensive, however, so only wealthy individuals can benefit from this private regulation of information flow: Without a right to be forgotten, ordinary people are at the mercy of the algorithms.

Online identity—the profile that emerges when online information connected to a person's name or other identifier is aggregated and made available to others—has increasingly become a central component of our social and professional lives. Youth are increasingly being taught about 'self-branding' as an important part of educational and professional success: They understand

---

27. Bennett et al, *supra* note 24 at 55-69.
28. See Kerry Maxwell, "Buzzwords: Egosurfing" (30 April 2004), *Macmillan Dictionary* (blog), online: <www.macmillandictionary.com/buzzword/entries/egosurfing.html>.
29. For up to date statistics on search engine market share by country or worldwide, see Global Stats, "Browser Market Share Worldwide" (January 2018), online: <gs.statcounter.com/search-engine-market-share>.
30. Randall Stross, *Planet Google: One Company's Audacious Plan to Organize Everything We Know* (New York: Free Press, 2008).
31. Alexander JAM van Deursen & Jan AGM van Dijk, "Using the Internet: Skill related problems in users' online behavior" (2009) 21:5&6 Interacting with Computers 393.
32. Search Engine Land, "What is SEO/Search Engine Optimization," online: <searchengineland.com/guide/what-is-seo>; Mayer-Schönberger, *supra* note 2 at 220-21; Jeffrey Rosen, "The Web Means the End of Forgetting," *The New York Times* (21 July 2010), online: <www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all>.

that online identity is central to many forms of social evaluation.[33] Lisa Austin described privacy as the regime by which we secure and bolster the conditions for self-formation and presentation, online and off. She argued that data protection principles establish the ground rules for creating and safeguarding an identity-favourable environment.[34] The problem with pervasive surveillance, then, is its possible effects on identity formation, revision, and tailoring to suit various social interactions.[35] It can stifle one's capacity to express "yourself freely in the here and now."[36] Erving Goffman noted that every individual has multiple identities, and that social interaction is built on which 'face' is put forward in a particular relational context.[37] With the explosion of data collection from so many different directions and via so many channels, we have been rapidly losing the capacity to meaningfully influence, much less control, this process.[38] The right to be forgotten, in its various forms, has the goal of allotting data subjects greater control over the flow of information about them.[39]

This article explores what a Canadian variant of the right to be forgotten might look like in relation to search engines as a particular type of business that collects and packages publicly available personal information about individuals.[40]

---

33. Alice E Marwick, *Status Update: Celebrity, Publicity, and Branding in the Social Media Age* (New Haven: Yale University Press, 2013).
34. Lisa M Austin, "Privacy and Private Law: The Dilemma of Justification" (2010) 55:2 McGill LJ 165.
35. danah boyd, *It's Complicated: The Social Lives of Networked Teens* (New Haven: Yale University Press, 2014).
36. Koops, *supra* note 7 at 233, cited in Antoinette Rouvroy, "Réinventer l'art d'oublier et de se faire oublier dans la société de l'Information? version augmentée du chapitre paru, sous le même titre" in Stéphanie Lacour, ed, *La sécurité de l'individu numérisé Réflexions prospectives et internationales* (Paris: L'Harmattan, 2007) 249 at 271-72.
37. Erving Goffman, *Interaction Ritual: Essays In Face-To-Face Behavior* (Chicago: Aldine Publishing Company, 1967); Austin, *supra* note 34; Vincent Miller, "A Crisis of Presence: On-line Culture and Being in the World" (2012) 16:3 Space & Polity 265.
38. Social media platforms, especially Facebook, have attempted to address their users' concerns about losing control over their online identity by creating simple tools like being able to "untag" one's photo someone else has posted. See Norberto Nuno Gomes de Andrade, "Oblivion: The Right to be Different…from Oneself: Re-proposing the Right to Be Forgotten" in Alessia Ghezzi, Ângela Guimarães Pereira & Lucia Vesnić-Alujević, eds, *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* (New York: Palgrave Macmillan, 2014) 65.
39. Forde, *supra* note 10 at 93; Orla Lynskey, "Deconstructing Data Protection: The 'Added Value' of a Right to Data Protection in the EU Legal Order" (2014) 63:3 ICLQ 569 at 581; Powles, *supra* note 3 at 585.
40. For a more in-depth discussion of privacy in publicly accessible information in Canada, see Andrea Slane, "Information Brokers, Fairness, and Privacy in Publicly Accessible Information" 4 Can J Comp & Contemp L [forthcoming in 2018] [Slane, "Information Brokers"].

Part I will consider the different versions of this 'right' in the EU, specifically obscurity, oblivion, and erasure. In particular, it will explore how the EU deals with publicly and indirectly collected information, given that until now data protection regimes generally have not regulated the collection and processing of such information. Part II will consider the digital information dynamics related to publicly available personal information, and what the normative impetus behind regulating these information dynamics might be. It will include a discussion of the difference between what search engines do and what news sources do, and how it may be possible to restrict the former while preserving the importance of expression and access to information regarding the latter. Part III explores the possibility of dividing publicly available personal information into three subcategories: information that should not have been published in the first place; information that is publicly available from public sector sources, but to which public access has been legitimately restricted; and information that, while legitimately and publicly available, has been given more prominence than warranted by way of a search engine's algorithm. Also important is whether this information has caused the data subject some harm.[41] It also considers the current Canadian approach to each of these categories, and explores how the right to be forgotten might fit into our already established or developing normative approaches to personal information flow. Part III concludes by suggesting a creative solution to the especially complex and novel dynamics of information flow.

I. VERSIONS OF THE RIGHT TO BE FORGOTTEN: OBSCURITY, OBLIVION, ERASURE

The idea of the right to be forgotten has been around for a couple of decades even in Canada,[42] but it blossomed into public consciousness in North America

41. Canadian scholars tend to require that a complainant demonstrate harm caused by the accessibility of the information in order to justify obscurity or erasure. This is not a requirement in the EU regulation. See Geneviève Saint-Laurent, "Vie privée et «Droit à L'oubli »: Que Fait Le Canada?" (2015) 66 UNBLJ 185 at 195; Gratton & Polonetsky, *supra* note 13.
42. In the latter part of the 1990s, the British Columbia Information and Privacy Commissioner mentioned the "right to be forgotten" in at least two rulings. See Office of the Information and Privacy Commissioner of British Columbia, *Inquiry RE: A decision by the Ministry of Finance and Corporate relations to withhold the names and addresses of property owners from copies of Certificates of Forfeiture* (6 March 1998), Order No 217-1998, online: OIPC <www.oipc.bc.ca/orders/438>; Office of the Information and Privacy Commissioner of British Columbia, *Inquiry RE: A decision by the Victoria Police Department to sever information and withhold law enforcement records from an applicant* (12 October 1995), Order No 58-1995, online: OIPC <www.oipc.bc.ca/orders/405>.

after the 2014 decision of the Court of Justice of the European Union ("CJEU") *Google Spain SL, Google Inc v Agencia Española de Protección de Datas (AEPD), Mario Costeja González*.[43] The nature of the right to be forgotten which emerges from that decision is fairly narrow. It identifies in what circumstances a data subject may demand that an information location service (*i.e.*, a search engine) de-link certain search results for a subject's name.[44] This version of the right is more accurately described as a right to obscurity: The content at issue remains available at the source, and may be located using other search terms.

Following the *Google Spain* decision, the EU proposed explicitly enshrining the right to be forgotten in a revision of its data protection directive. EU Commissioner Viviane Reding described this move as merely making an existing right clearer, rather than creating a new right.[45] However, it remains unclear as to how the new regulation will apply to search engines.[46] The new General Data Protection Regulation ("GDPR") applies as of 25 May 2018, and includes a right to erasure—also referred to as a right to be forgotten—which enables data subjects to request erasure of their personal information held by data controllers under a list of circumstances, and subject to a list of exceptions.[47] This newly specified right is the right to have information deleted at the source. It strengthens existing obligations for data controllers who privately collect

43. *Google Spain, SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, C-131/12, [2014] ECR I-317 [*Google Spain*].
44. Julia Kerr has expressed concern that the *Google Spain* decision did not adequately define the meaning of search engine. She explains the importance of distinguishing between general search engines such as Google from internal search engines such as court or government websites. See Julia Kerr, "What is a Search Engine? The Simple Question the Court of Justice of the European Union Forgot to Ask and What It Means for the Future of the Right to Be Forgotten" (2016) 17:1 Chicago J Intl L 217 at 221.
45. Viviane Reding, "The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age" (Address delivered at the Digital-Life-Design Conference, Munich, Germany 22 January 2012), online: European Commission Press Release Database <europa.eu/rapid/press-release_SPEECH-12-26_en.htm>.
46. *Ibid*. Reding describes the right to be forgotten in terms of consent and control: "If an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system." Determining what constitutes "legitimate reasons" for keeping information accessible is a more complex process when it comes to the information publicly available on search engines as compared with data that was provided directly by a customer to a business.
47. EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 17 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art 17 [*GDPR*].

consumer information, but also appears to apply in some measure to publicly collected information.[48]

In tracing the origins of rights to obscurity or erasure, several scholars have cited the longer-standing continental European tradition of a 'right to oblivion,' which is a strongly enforced version of a 'clean slate' policy for certain past mistakes.[49] Mostly, the right to oblivion relates to criminal history information that is prohibited from being republished after individuals have resolved their entanglement with the justice system.[50] Various European countries have suppressed factual publications (news articles, documentary television programs, films, et cetera), upon complaints by the offender or the offender's family that reviving information about past crimes impinges on the rights of the offender.[51] While many jurisdictions have some variation of clean slate policies for certain past events, the information about these past events continues to reside at its original official source, so it is not truly 'erased' the way that privately collected information might be. The right to oblivion is therefore something other than a right to erasure, dealing specifically with suppressing wider publication of outdated information housed in public records: It is perhaps more accurately a hybrid of erasure and obscurity, as elaborated below.

A. OBSCURITY

The *Google Spain* case began in 2009 when the complainant, Mario Costeja González, sought to suppress archived announcements from 1998 that publicized forced auctions of his properties to satisfy social security debts.[52] The announcements, somewhat inexplicably, appeared prominently on searches for his name, and so he asked the newspaper that housed the announcements in its online archive to delete them; when it refused, he asked Google to de-link

48. So far, Google has implemented the more limited holding in *Google Spain* to deal with requests to alter search engine results linked to a data subject's name. The company rejects over half of the requests they receive. It remains to be seen whether the new regulation will change how search engines are expected to respond to requests, and how much it would disrupt the balancing of interests in publicly available information that Google has thus far maintained.
49. Saint-Laurent, *supra* note 41; Cofone, *supra* note 10 at 2; Ambrose, *supra* note 10 at 380-81; Forde, *supra* note 10 at 85.
50. Werro, *supra* note 13.
51. *Ibid* at 290-91. Werro discusses several of these cases including *AG v W*, BGE 122 III 449 (1996) and *A v Journal de Genève et de la Gazette de Lausanne*, 23 10/2003, 5C156/2003 (2003).
52. *Google Spain*, *supra* note 43 at para 14.

the archives from searches of his name.[53] When Google also refused, Costeja González complained to the Spanish data protection authority ("AEPD"), which denied his complaint against the newspaper but supported his complaint against Google.[54] Google appealed to the *Audiencia Nacional* (National High Court of Spain) which stayed proceedings in order to request that the CJEU rule on key preliminary questions, including whether the Data Protection Directive[55] applies to search engines when they gather publicly available information from the Internet, and if so, under what circumstances a search engine would be required to cease processing personal information collected that way.[56]

The CJEU determined that Google does collect personal data through its web crawlers and processes the information through its algorithms:

> Therefore, it must be found that, in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine "collects" such data which it subsequently "retrieves," "records" and "organises" within the framework of its indexing programmes, "stores" on its servers and, as the case may be, "discloses" and "makes available" to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as "processing" within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data.[57]

Interesting in this conclusion is that the CJEU did not accept Google's argument that its automated web crawlers do not distinguish between personal and other information and do not assert any influence over the content available on third-party sites, and so Google should not be considered to 'control' the personal data it gathers. The CJEU instead found that Google is in fact a 'data controller' for the purposes of the Data Protection Directive, because it determines both the purpose and the means of processing the personal data that it collects and packages via its algorithms and monetizes this process by selling advertising related to that collated and packaged personal information.[58]

---

53. *Ibid* at para 15.
54. *Ibid* at paras 16-17.
55. EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281 [*Data Protection Directive*]. The *Data Protection Directive* was repealed by *GDPR*, *supra* note 47.
56. *Google Spain*, *supra* note 43 at para 20.
57. *Ibid* at para 28.
58. *Ibid* at paras 32-33. For discussion see David Hoffman, Paula Bruening & Sophia Carter, "The Right to Obscurity: How We Can Implement the *Google Spain* Decision" (2016) 17:3 NCJL & Tech 437 at 447-48; Saint-Laurent, *supra* note 41.

Ultimately, the CJEU determined that upon request by a data subject, search engines must remove "inadequate, irrelevant, no longer relevant or excessive"[59] information generated upon a search of a person's name unless there is a public interest in retaining the link to that information.[60] The CJEU considered the specific role that search engines play in processing personal data: Both in terms of locating information about the data subject that users would have far more difficulty finding by other means[61] and in terms of creating and delivering an online profile of the data subject to users (*i.e.*, "obtaining through the list of results a structured overview of the information relating to that individual that can be found on the Internet enabling them to establish a more or less detailed profile of the data subject").[62] The court found that the unique effect of this compiled list of results is potentially greater than any one result contained on the list, because the list as a whole:

> [P]otentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty—and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous.[63]

In Canada, the type of information that would be eligible for de-listing from a person's name search would be evaluated with respect to the principles of accuracy, purpose, and consent, along with the overarching requirement of reasonableness, rather than relevance, adequacy, or excessiveness, which are terms that *PIPEDA* does not share with the *Data Protection Directive*. The accuracy principle requires that "[p]ersonal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used," and the OPC has taken the position that this principle applies to search engines, signifying that data subjects have a right to challenge the accuracy, completeness, and currency of personal information and to have this information amended where it is inaccurate, incomplete, or out of date.[64] The OPC also proposes that the appropriate purposes principle should apply,[65] and that:

---

59. *Google Spain*, *supra* note 43 at paras 92-94. The terms in the *Google Spain* decision are drawn from the *Data Protection Directive*. See *Data Protection Directive*, *supra* note 55, art 6.
60. *Google Spain*, *supra* note 43 at paras 81, 97.
61. *Ibid* at para 36.
62. *Ibid* at para 37.
63. *Ibid* at para 80.
64. *PIPEDA*, *supra* note 4, Schedule 1, Principle 4.6; OPC*, Draft OPC Position*, *supra* note 4.
65. *PIPEDA*, *supra* note 4, s 5(3).

> [T]here 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.[66]

The regulation governing the publicly available information exception to the consent requirement[67] also pivots on the purpose for which that information was collected, used, or disclosed. Publicly-available information (meaning, generally, information originating or housed in a public sector source) can be collected, used, or disclosed without consent only where this further collection, use, or disclosure of the personal information relates directly to the purpose for which the information originally appears in the directory, listing, notice, registry, record, or document in which it was found.[68] The OPC and the Federal Court denied the shelter of this exception to Globe24h, reasoning that as a commercial website whose interest was primarily in profit, it did not disclose the personal information it collected from publicly available legal databases for a purpose directly related to the original purpose for which a litigant has given consent—namely in the spirit of the open court principle.[69] This reasoning could be extended to consider whether personal information that has been made publicly available complies with the appropriate purposes principle to begin with, as will be elaborated on in Part III below.

In Canada, expectations of privacy, including expectations with regard to data protection, must be reasonable.[70] The purpose provision of *PIPEDA* brings this home: "[I]n an era in which technology increasingly facilitates the circulation and exchange of information," *PIPEDA*'s purpose is to provide:

> rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal

66. OPC*, Draft OPC Position*, *supra* note 4.
67. *PIPEDA*, *supra* note 4, ss 7(1)(d), 7(2)(c.1), 7(3)(h.1).
68. *RSPAI*, *supra* note 5, ss 1(a)-1(d); More controversially, this regulation limits the "publicly available exception" where the information appears in a publication (including a magazine, book or newspaper). This makes it more difficult to collect, use, and disclose personal information even when the renewed disclosure relates directly to the purpose for which the information originally shared. As a result of the fact that there is an additional exception for the collection, use, and disclosure of personal information for journalistic, artistic, or literary purposes, this regulation addresses information shared for different reasons (*ibid*, s 1(e)).
69. *Globe24h*, *supra* note 5.
70. Andrea Slane & Lisa M Austin, "What's In a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57:4 Crim LQ 486.

> information for purposes that a reasonable person would consider appropriate in the circumstances.[71]

These circumstances could include collection and collation of publicly available information along the lines of the CJEU's reasons, and a "reasonable person" standard in relation to such an activity could translate into what is normatively appropriate to include in search results of publicly available materials, broadly understood. A fuller analysis of how such a normatively appropriate standard might be crafted—having regard to the freedom of expression interests not just of the organizations subject to *PIPEDA* but more importantly the users of their service—will need to consider what may be different about the kind of personal information collection that search engines do. As the OPC acknowledges, it is clearly not appropriate to require a search engine to abide by *all* of the *PIPEDA* requirements.[72] However, it may well be appropriate to require the search engine to address particular problems with personal information flows that are created or exacerbated by the search engine's presentation of search results.[73]

This is clearly not how search engines currently work. Indeed, Google's algorithms do not currently consider the purposes for which consent may or may not have been given when they collect and collate public websites containing personal information, but are instead focused on meeting expectations of relevance for users and clients (*e.g.*, advertisers). Google tailors its search results to users depending on previous searches, so a user who has previously shown an interest in, for example, humiliating information about people who clearly never consented to its publication, will likely find it again. If the point is to balance privacy with Google's business interests in delivering what people are looking for, whether it is *normatively* reasonable for a person to be able to easily locate humiliating information about a person is a different question. Google's decisions about which requested search removals under European privacy law to honour and which to deny are made by real people, not algorithms, so these decisions are better able to accommodate normative expectations.[74] This normative approach is what the CJEU aimed for in *Google Spain*, in that the nature of the public interest at stake is very specific: It is not whether the public interest is served by

71. *PIPEDA*, *supra* note 4, s 3.
72. *OPC Consent Report*, *supra* note 9 at 15-16; Michael Rosenstock, "Is there a 'right to be forgotten' in Canada's *Personal Information Protection and Electronic Documents Act (PIPEDA)*?" (2016) 14:1 CJLT 131 at 147.
73. *Ibid* at 151.
74. Google Transparency Report Help Center, "European privacy requests Search removals FAQs," online: <www.google.com/transparencyreport/removals/europeprivacy/faq> at FAQ: "Who makes decisions about requests to delist content?" [*Google FAQs*].

the existence of the information, but whether it is in the public interest that the information remains accessible by searching the data subject's name.[75]

Google has developed parameters for deciding what sorts of search removal requests to honour according to the Article 29 Working Party guidelines.[76] It uses a four-step evaluation process, the most difficult questions being: "Does the page requested for removal include information that is inadequate, irrelevant, no longer relevant, or excessive, based on the information that the requester provides? Is there a public interest in that information remaining available in search results generated by a search for the requester's name?"[77]

The specifics of this evaluation process, like the algorithm by which the information turns up in the first place, are shrouded in mystery. Nonetheless, Google has disclosed that common scenarios for delisting pages are a "clear absence of public interest," "sensitive information," "content relating to minors," and "spent convictions/exonerations/acquittals for crimes."[78] Requests have involved a wide range of websites, with the top ten sites accounting for only a fraction of requests (Facebook is the top site, and none of the top sites is a traditional news outlet).[79] With regard to traditional news content, Google provides examples of requests it has honoured and requests it has rejected, making it apparent that it will generally grant requests made by private individuals in relation to minor incidents (including minor, long ago crimes), but not those made by public figures or people who have abused the public's trust (*e.g.*, by professional

75. *Google Spain*, *supra* note 43 at para 97. See OPC, *Draft OPC Position*, *supra* note 4 (demonstrating that the OPC has adopted this approach in its proposed position: "[T]he 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").
76. Article 29 Data Protection Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González' C131/12" WP 225 (adopted 26 November 2014), online: <www.dataprotection.ro/servlet/ViewDocument?id=1080> [*WP29 Guidelines*].
77. *Google FAQs*, *supra* note 74 at FAQ: "How do you evaluate requests?".
78. *Ibid* at FAQ: "What are some common scenarios for delisting pages?".
79. Google, "Transparency Report: Search removals under European privacy law," (accessed on 16 April 2018), online: <www.google.com/transparencyreport/removals/europeprivacy> [Google, "Transparency Report"].

misconduct), and not those involving major crimes or incidents.[80] Google has processed hundreds of thousands of requests, and has honoured fewer than half of these.[81] Very few decisions not to remove links have been appealed by the data subject, so the decisions do not appear to be outrageously out of line.[82]

The right to obscurity—in the form of de-listing certain search results from a search of a person's name through a data protection regime—involves balancing multiple interests: Those of the data location business (Google) and the data subject, but also potentially of the source content providers, and the public who use the data location services. The latter two interests generally do not come into play when regulating how businesses privately and directly collect and process personal information from their customers, so the balancing required to be "reasonable" in the Canadian context under *PIPEDA* will evolve in that it will need to better accommodate freedom of expression interests.[83] Canadian courts have considered freedom of expression interests in the information on websites, and at least in the indirect role of search engines (like Google) in finding it: None of those cases precludes the implementation of a more tempered version of the right to be forgotten, rooted in modifying the application of *PIPEDA* such that it is more attentive to freedom of expression.[84]

In the wake of *Google Spain* in the EU, it is clear that there are ways to devise a right to be forgotten that would take a broader set of interests into consideration (search engine, data subject, content provider, and user). Google has taken voluntary steps to enhance the balancing of interests in their removal request process. For example, it has chosen to implement a notification practice to inform source content providers that a URL has been de-listed. Such notification is not required by EU data protection law, but the Article 29 Working Party acknowledged that search engines may choose to do so, provided

---

80. *Ibid*. The OPC has similarly come up with a distilled list of factors to consider when assessing whether the algorithm has failed to appropriately balance a data subject's privacy with the public interest in maintaining easy access to particular results, namely: whether the individual is a public figure, and whether the information relates to a matter of public controversy or debate, an individual's private or professional life, a criminal offence for which an individual received a discharge, pardon or record suspension, or information relating to a minor. See OPC, *Draft OPC Position*, *supra* note 4.
81. Google has processed 669,848 requests pertaining to 2,488,228 URLs and has removed 43.9% of these. See Google, "Transparency Report," *supra* note 79 (accessed on 16 April 2018).
82. Powles, *supra* note 3 at 602.
83. Rosenstock, *supra* note 72 at 150.
84. *Globe24h*, *supra* note 5; *Google Inc v Equustek Solutions Inc*, 2017 SCC 34, [2017] 1 SCR 824 [*Equustek*]; *Crookes v Newton*, 2011 SCC 47, [2011] 3 SCR 269 [*Crookes*].

that the notifications do not identify who made the request.[85] This practice has drawn some criticism as news agencies have jumped to conclusions, sometimes incorrectly, about which person's name has been de-listed.[86] Google also allows webmasters to ask for re-review of its decision to de-list a URL, although this too is not required by the data protection regime.[87] Implementing a process for de-listing publicly available information in Canada—especially information that is lawfully published—would require a means for a content provider to complain and escalate a complaint, similar to the complaint process available to data subjects under *PIPEDA*.

The freedom of expression interests of search engine users have so far not been straightforwardly accommodated in the implementation of the European right to be forgotten. Google suggested that users should be notified when their search results may have been altered due to privacy requests,[88] although such notification is inconsistent with Google's current model whereby users are not informed of Google's own editing and manipulating of search results. Google's existing search alteration practices and policies remain a strong argument against Google's claim that it is merely providing a list of sites publicly available on the web and that tampering with it would impinge upon the right of users to access that information.[89] Indeed, private companies' culling objectionable material—much of it not illegal—from search results or news feeds is a sticky problem for freedom of expression online. Private companies are not held to constitutional standards of freedom of expression, and indeed their success in part depends on their capacity to avoid delivering shocking or distasteful content to users who do not actively choose to see such material.[90] With regard to search results in particular, the user perspective is also difficult to entirely integrate with the

85. *WP29 Guidelines*, *supra* note 76 at 2-3, 7.
86. Powles, *supra* note 3 at 597-98.
87. *Google FAQs*, *supra* note 74 at FAQ: "Do webmasters have any way of challenging your decisions?".
88. Christopher Berzins, "The Right to be Forgotten After Google Spain: Is it Coming to Canada?" (2015) 28:3 Can J Admin L & Prac 267 at 270.
89. *Equustek*, *supra* note 84 (Factum of the Appellant at para 24), online: <www.scc-csc.ca/WebDocuments-DocumentsWeb/36602/FM010_Appellant_Google-Inc.pdf> [*Equustek* FOA]; *Equustek*, *supra* note 84 (Factum of the Respondent at para 22), online: <www.scc-csc.ca/WebDocuments-DocumentsWeb/36602/FM020_Respondent_Equustek-Solutions-Inc.pdf> [*Equustek* FOR]; *Equustek*, *supra* note 84 at para 50 (demonstrating that the SCC sided with the respondent: "[Google] acknowledges, fairly, that it can, and often does, exactly what is being asked of it in this case, that is, alter search results").
90. Kyle Langvardt, "Regulating Online Content Moderation," 106:5 Geo LJ [forthcoming in 2018].

algorithmic logic of delivering the most 'relevant' results with a right of access to information. In putting forth a theory that search engines operate as 'advisors' rather than as mere conduits or more active editors, James Grimmelman states, "[f]rom a user's perspective, relevance is a subjective goal. But from a search engine's perspective, search rankings are approximations of objectively but imperfectly observable characteristics of subjective user preferences, embodied in the search engine's choices about its algorithms."[91] Users are therefore never entitled to any results in particular, only the list of sites that the search engine has compiled in its imperfect estimation of what the user is looking for.

Of course, a private company's choice to restrict access to certain information is not subject to the *Charter* the way that government-mandated restriction of that information would be. Application of *PIPEDA* would have to be justified under section 1 of the *Charter* which would require sufficient clarity about how *PIPEDA* would apply to the provision of search results. As a service that presents advice to users as to what sites they might find relevant to their search needs, the search engine might also assert its own speech rights as connected to the rights of users, as Google argued in *Equustek*:

> The injunction directly limits both Google's speech (by prohibiting it from truthfully reporting to users the existence of publicly accessible websites) and that of the public (by preventing them from using Google's search engine to find and access information that is publicly available on the Internet). The fact that there may be a justification for limiting the *Defendants'* speech should not allow a court to order Google, or any search engine, to inaccurately report the non-existence of a website that remains on the Internet.[92]

However, the general argument that no legal mechanism can compel a search engine to de-list or de-index certain search results and still be *Charter*-compliant was rejected by the Supreme Court of Canada ("SCC"). The Court concluded that issuing a preliminary injunction ordering Google to de-index the websites of the defendant company, whereby it persistently infringed the intellectual property rights of the plaintiff, was not contrary to anyone's freedom of expression interests—The analysis of *PIPEDA*–based privacy requests to de-list links is therefore likely to similarly depend on the expression interests at stake in a given request or category of requests, as per the typology set out in Part III below.[93]

---

91. James Grimmelmann, "Speech Engines" (2014) 98:3 Minn L Rev 868 at 915.
92. *Equustek* FOA, *supra* note 89 at para 27 [emphasis in original].
93. *Ibid* at paras 48-49.

B. OBLIVION

While the additional applications of a data subject's right to control their personal information in the EU may seem new, many scholars have pointed to the *droit à l'oubli* and related rights in some European countries as a longer tradition informing a right to suppress publication of especially 'outdated' information. The passage of time is one factor that might make publicly accessible information no longer relevant and thus subject to a right to oblivion—a somewhat stronger variant of the right to obscurity. In Europe, this right means that in some jurisdictions public mention of a person's criminal history, for example, is an actionable wrong unless there are compelling public interest reasons to revive publicity of these past wrongs.[94] However, the right to oblivion is not a right to complete erasure. As with most 'clean slate' policies, a record of past wrongs (or financial troubles, such as bankruptcies) continues to exist, usually in a government database, which may allow public access, though often on a restricted basis.

As applied in the EU, the *droit à l'oubli* obliges search engines, including news sites, to de-index or de-list sites that mention spent criminal convictions, except where the public interest requires retaining easy public access to that information. Google has posted examples of its practice of de-listing sources from name searches to news sources that reference minor past criminal convictions, but Google does not appear to have wholly de-indexed any sites referencing past convictions. This obligation is complicated by divergent understandings of what search engines are doing when search results include an old news story (or an old announcement, as was the case in *Google Spain*): Are they republishing that information anew, thereby reviving interest in the outdated information? Or are they merely pointing to a historical source?

Google regularly argues that it is presenting neutral reference to the existence of websites that house this information, including, as noted above, in *Equustek*. Julia Powles issued a strong critique of that line of argument in *Google Spain*, that interfering with search results would distort truth, history, and public memory.[95] Powles asserted that search engines and other Internet service providers have long capitalized on the perception that the Internet is a public sphere, or a vast public archive, when really it has always been a network of privately owned and controlled networks.[96] These privately owned networks are designed to benefit these companies. What does or does not remain publicly available should not

94. Werro, *supra* note 13 at 291.
95. Powles, *supra* note 3 at 585.
96. *Ibid* at 591.

be equated with the value we place in true public records and archives that are important to the democratic pillar of transparency and preservation of history.[97]

Canada's access to information regime balances the right to access government information with privacy rights on a regular basis, and continually adjusts and refines the parameters of this balance. In *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, the SCC affirmed lower court rulings and the finding of Ontario's Information and Privacy Commissioner ordering release of the requested information, holding that the personal information exemption did not apply because the information did not present a reasonable risk of being connected with a particular individual (here, release of data regarding the number of registered sex offenders residing within areas captured by the first three digits of Ontario postal codes).[98] Amy Conroy and Teresa Scassa, however, argue that the SCC was perhaps too confident that this information will remain de-identified in the age of data mining, and suggested instead that decisions on whether to release government-held personal information should rest on whether the release expressly furthers the values of transparency and accountability.[99] In other words, a decision about public release of information should be justified by its purpose (here, being in the service of government transparency and accountability), rather than confusing release of information itself with transparency and accountability.

Canadian information policy has also recognized that not all sensitive personal information should be held in archives, no matter how historically significant the context in which that information was initially recorded may be.[100] In *Canada (Attorney General) v Fontaine*, survivors of abuse in government-sponsored residential schools had been promised confidentiality of the highly sensitive personal information they provided in the course of the Independent Assessment Process under the Indian Residential Schools Settlement Agreement. Despite strong advocacy by the Canadian National Archive and others that this testimony should be preserved and retained in a protected archive, the Court ruled that the affected individuals had a right to choose whether to have records of their testimony preserved or destroyed.[101]

---

97. *Ibid*.
98. *Ontario (Community Safety and Correctional Services) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 31 at paras 59-66, [2014] 1 SCR 674.
99. Amy Conroy & Teresa Scassa, "Promoting Transparency While Protecting Privacy in Open Government in Canada" (2015) 53:1 Alta L Rev 175.
100. *Canada (Attorney General) v Fontaine*, 2017 SCC 47, [2017] 2 SCR 205.
101. *Ibid* at para 62.

Certainly, Canadian freedom of expression jurisprudence does not support prohibitions on republishing or reviving interest in past events, and imposing any such prohibitions on news archives or on returning search results related to news archives would surely violate section 2(b) of the *Charter*. However, Canadian information access policy is more nuanced about the balance between privacy and public access to information, indicating that some form of obscurity or oblivion for access to records of past events may well be in keeping with broader normative values regarding information flow.

C. ERASURE

The new EU General Data Protection Regulation 2016/679 explicitly sets out a "right to erasure" which it also labels as a "right to be forgotten," terminology which might fan the flames of concerns about "rewriting history."[102] The regulation creates a substantive right for a data subject to request removal of personal data from data controllers for a list of circumstances. Some of these involve violation of existing data protection principles, including where personal information is no longer necessary in relation to the purpose for which is was collected, where the data subject withdraws the consent on which processing was based, and where the personal information was unlawfully processed.[103] In these circumstances, the right to erasure adds a direct remedy for data subjects in addition to existing constraints on business use of information collected from customers. The right to erasure also applies where the data subject objects to processing of their data.[104]

The right to object applies to all processing of data, including the kind of processing involved in "big data" analytics as well as the processing of publicly accessible data by a search engine. Overall, the regulation stresses balancing the interests that must be considered in granting erasure, stating that lawful data processing includes where "processing is necessary for the performance of a task carried out in the public interest," and where:

> processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.[105]

---

102. *GDPR*, *supra* note 47, art 17; Will Gore, "The Only Way is Ethics - Is the 'right to be forgotten' being used to rewrite history?" *The Independent* (15 November 2015), online: <www.independent.co.uk/voices/the-only-way-is-ethics-is-the-right-to-be-forgotten-being-used-to-rewrite-history-a6735346.html>.
103. *GDPR*, *supra* note 47, art 17.
104. *Ibid*, art 21.
105. *Ibid*, art 6(1)(e)-(f).

Article 17 further reiterates that the right to erasure will not apply where the processing is necessary to exercise a competing right, including freedom of expression and information, performance of a task carried out in the public interest, processing in the service of archiving in the public interest, or historical, scientific or statistical research purposes "where erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing."[106]

For search engines, erasure is actually "de-indexing." Unless the right to erasure is successfully enforced against the actual source of the content, the personal information remains at the source, but ceases to be returned in any search results on that search engine's service. This form of erasure—as implemented by an information location service—is actually more a form of hyper-obscurity, in the sense that while the information continues to exist at the source, it can no longer be found through the search engine. In order to locate the information, it would be necessary to know the URL and enter it into a browser. Therefore, the right to erasure and its search engine variant of complete de-indexing is a means to bolster existing data protection principles that support the autonomy rights of data subjects, but extends that protection to a broader range of data processing practices: Profiling of online users ("big data" gathered from public online activity) and where publicly accessible information is being collected, collated, and presented for ease of access.

In Canada, the question of whether ordering Google to de-index a specific site would be "just and equitable in all the circumstances of the case" was the key issue on the appeal in *Equustek*.[107] Since that case dealt with a preliminary injunction, the Court only commented on its capacity to issue an order compelling a non-party (Google) to cease facilitating the harm caused by the defendant's site, noting that without a court order Google would continue to facilitate that harm.[108] Making search engines subject to *PIPEDA* in a way that might require de-indexing of certain sites is a related but not identical question. This question is not so much focused on the search engine's uninvolved facilitation of access to content (though the nature of that content is of course highly relevant to the determination of whether to de-list, de-index, or refuse a request to do so), but rather is focused on the information product that the search engine itself provides (namely, the search result list). That is, it imposes data protection obligations on the 'advice' the search engine provides as to which sites a user may find relevant. The results list is itself subject to regulation in the EU as a source, not

106. *Ibid*, art 17(3).
107. *Equustek*, *supra* note 84 at para 1.
108. *Ibid* at para 35.

just as providing neutral reference to other impugned sources, and Canada could similarly obligate search engines to de-index sites because pointing users to those sites would in itself be a contravention of *PIPEDA*.

This brings us back again to the question of whether search engines have expression rights—including whether those rights primarily stem from the rights of their users to hear whatever expression the search engine is entitled to produce. In *Equustek*, Google drew on the SCC's reasoning in *Crookes v Newton* that providing hyperlinks engages freedom of expression and should not incur liability for linking to defamatory content without more active promotion by the speaker. Google argued that the list of hyperlinks generated by search engine results are protected speech such that, expanding on *Crookes*, any restrictions on providing hyperlinks would intolerably undermine the ability of the Internet to function,[109] and would impinge on the "the public's right to access information."[110] Presenting hyperlinks in search results, so the argument goes, should be immune from legal regulation, because, as the SCC ruled in *Crookes*, "[m]aking reference to the existence and/or location of content by hyperlink or otherwise, without more, is not publication of that content,"[111] and, "[t]he Internet cannot, in short, provide access to information without hyperlinks. Limiting their usefulness by subjecting them to the traditional publication rule would have the effect of seriously restricting the flow of information and, as a result, freedom of expression."[112] The SCC's ruling in *Crookes,* however, and these passages in particular, apply to "publication" as understood in defamation law: That is, whether the person providing the hyperlink is a "publisher" and hence liable for disseminating defamatory content. A finding that simply providing a hyperlink is not "publication" in this sense does not translate into blanket immunity from legal regulation of all hyperlinking practices. If *Crookes* were to be interpreted that broadly, then Google and other search engines would never be subject to any legal constraints regarding links, which is clearly not the case in Canada, especially after the SCC ruling in *Equustek*.[113]

According to the Article 29 Working Party, a key holding of the CJEU in the *Google Spain* decision is that "[t]he processing of personal data carried out in the context of the activity of the search engine must be distinguished from, and

---

109. *Equustek* FOA, *supra* note 89 at paras 30-32.
110. *Ibid* at para 41.
111. *Crookes*, *supra* note 84 at para 42, cited in *Equustek* FOA, *supra* note 89 at para 30.
112. *Crookes*, *supra* note 84 at para 36.
113. Equustek also makes this point in its factum on appeal. See *Equustek* FOR, *supra* note 89 at para 104.

is additional to that carried out by publishers of third-party websites."[114] While there are separate considerations for different kinds of content hosts regarding the right to be forgotten and freedom of expression—especially news sources[115]—search engine results should be subject to analysis according to what they are (a list of materials Google has compiled in relation to a search term entered by a particular user) not only in reference to the content they refer to.

The three "right to be forgotten" options really boil down to two main possibilities: obscurity of varying degrees (de-listing particular results connected to a person's name, or de-indexing content entirely) and erasure (deleting information at its source). It is clear that the right to be forgotten as related particularly to search engines is not about imposing liability on information intermediaries as publishers. Instead, it is about assigning responsibility to participate in finding a solution for information flow problems that the service is responsible for creating or enabling. It is about rebalancing the values at stake in information flow: Certainly freedom of expression, transparency, and cultural memory, but also privacy, identity, and collective support for protecting vulnerable people from informational abuse and exploitation.[116]

II. ONLINE INFORMATION DYNAMICS, PERCEIVED POTENTIAL FOR HARM, AND THE RIGHT TO BE FORGOTTEN

Digital networked technology and the resulting changes to social interactions have produced anxiety or, at the very least, concern and trepidation about how personal information becomes and remains publicly available online. This anxiety is sometimes caused by exaggeration of the likely results, but it is clearly derived from disturbing possibilities. Five features of digital technology are particularly relevant to this discussion: (1) permanence, (2) easy accessibility, (3) vast audiences, (4) mysterious processes, and (5) uncontrollability. The various versions of the right to be forgotten address the perceived harmful impact of these five features, which, in combination with the overall principles of data

114. *WP29 Guidelines*, *supra* note 76 at 2.
115. Ivor Shapiro & Brian MacLeod Rogers, "How the 'Right to Forgotten' Challenges Journalistic Principles: Privacy, freedom and news durability" (2017) 5:9 Digital Journalism 1101.
116. Danielle Keats Citron, *Hate Crimes in Cyberspace* (Cambridge, Mass: Harvard University Press, 2014); Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: New York University Press, 2018).

protection and an appropriate balance with protection of access to information online, form the normative basis for providing such a right.

Fears about online permanence arise from the fact that once data is digital, it can be endlessly stored, duplicated, and circulated at almost no cost. The actual duration of online information available for access is unpredictable, with much of the information disappearing on a regular basis.[117] Nonetheless, the possibility of permanence has led to many public service campaigns warning youth that the Internet is 'forever' and to 'think before they post.'[118] These dire warnings intend to scare young people from taking risks with their online self-expression, but they also highlight a consequence of online permanence: Negative, embarrassing, or humiliating information that is permanently available can be exceptionally damaging to mental health.[119] This negative information blocks longstanding therapeutic methods for 'moving on' after a trauma, because the trauma never really fades into the past.

Self-interested Internet companies have also encouraged the idea of the permanence of online data. They claim that attempts to interfere with the flow of information online are ineffective because erasing or de-indexing one source does not mean that the information will not spring up again in another source. While this claim is true, it neglects the fact that a lot of information actually does not spring up elsewhere. Although erasing or de-indexing sites is not foolproof, it should be considered as, at most uneven, but not universally ineffective.[120] Any measure that disrupts the easy availability of negative information will help debunk the idea of permanence, lessen its impact, and thus have positive psychological effects on traumatized data subjects.[121]

The easy accessibility enabled by digital technology refers mainly to the success of services like Google, whereby information that might have been

---

117. Ambrose, *supra* note 10 at 372.
118. See *e.g.* Camille Webb, "Teen 'Sexting': Strike a pose. Press send. Regret it forever." *Health Leader* (14 May 2009), online: The University of Texas Health Science Center at Houston <www.uthealthleader.org/story/teen-sexting>.
119. Jennifer Martin, "Child Sexual Abuse Images Online: Implications for Social Work Training and Practice" (2016) 46:2 Brit J Soc Work 372; Keita Suzuki et al, "Cyberbullying and adolescent mental health" (2012) 24:1 Intl J Adolescence Med & Health 27; Ericka Adams, Elsa Y Chen & Rosella Chapman, "Erasing the Mark of a Criminal Past: Ex-Offenders' Expectations and Experiences with Record Clearance" (2016) 19:1 Punishment & Soc'y 23.
120. *Equustek* FOA, *supra* note 89 at paras 20-21.
121. Jennifer Martin, "Conceptualizing the Harms Done to Children Made the Subjects of Sexual Abuse Images Online" (2015) 36:4 Child & Youth Services 267 at 269-71 [Martin, "Conceptualizing the Harms Done"]; Andrea Slane, "Legal Conceptions of Harm Related to Sexual Images Online in the United States and Canada" (2015) 36:4 Child & Youth Services 288.

known to only a small circle of people can become a 'public fact' linked to a person by a name search.[122] Again, public service campaigns have often invoked the fear that a person who was not intended to gain access to certain information (*e.g.*, a grandmother or a potential employer) will be shocked by what they find online about you.[123] We now tend to judge people based on online information, leading to what some scholars refer to as an overall decline in the quality of human interactions as technology replaces in-person contacts.[124] While obscurity measures would not necessarily mitigate this trend, they could reinforce informational boundaries and protect contextual integrity by making some personal information harder to find again.[125]

The issue of easy accessibility was central to *Globe24h*. The commercial activities the site engaged in (such as selling advertising and charging fees to remove content from the site) were based on republishing court and tribunal decisions and allowing general search engines (*i.e.*, Google) to index them.[126] The Federal Court discussed how this business model, which capitalizes on people's desire to remain obscure despite knowing that their information is publicly available in legal databases,[127] did not comport with the open court principle to which most parties to court proceedings are deemed to have consented or at least through which they may be obligated to cede their privacy rights. Since the materials were already publicly available through free legal databases like CanLII (which do not allow their contents to be indexed by search engines), the Federal Court found that Globe24h merely violated the complainants' privacy by making their information easily locatable, even to people who were not specifically looking for it, without adding anything to the transparency and accountability undergirded by the open court principle. This case therefore stands for the idea that the values

---

122. Woodrow Hartzog & Frederic Stutzman, "The Case for Online Obscurity" (2013) 101:1 Cal L Rev 1 at 35; Allyson Haynes Stuart, "Google Search Results: Buried if Not Forgotten" (2014) 15:3 NCJL & Tech 463 at 473-74.
123. There are a number of online blogs that give advice to youth regarding their online profiles. See *e.g.* Vanderbilt, "Can it Pass the Grandma Test? 5 Social Media Tips" (Spring 2016), *Vanderbilt Business* (blog), online: <https://magazine.owen.vanderbilt.edu/can-it-pass-the-grandma-test-5-social-media-tips>.
124. See generally Sherry Turkle, *Alone Together: Why We Expect More from Technology and Less from Each Other* (New York: Basic Books, 2011); Sherry Turkle, *Reclaiming Conversation: The Power of Talk in a Digital Age* (New York: Penguin Press, 2015).
125. Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford: Stanford University Press, 2009) at 242; Mayer-Schönberger, *supra* note 2 at 181-82; Powles, *supra* note 3 at 598.
126. *Globe24h*, *supra* note 5 at paras 10-11, 32-37.
127. *Ibid* at paras 21, 23.

connected with access to information do not require easy (and hence possibly inadvertent) access.[128]

The vast audiences feature of digital technology refers to the unpredictable nature of online information flow, where anyone can pass on anything they have encountered to their whole list of online contacts or to the public at large. When something goes "viral," it has caught on to some hard-to-predict hook that inspires people to pass it on en masse.[129] A related digital phenomenon is the flourishing "subculture of humiliation," wherein viewing and commenting upon embarrassing photos or information about others (who are often strangers) has become a popular form of entertainment.[130] This can lead to anxiety about searches not only by friends, family, or peers, but also by strangers. The psychological consequence of feeling like 'everyone knows' about some sensitive personal information is another well-documented barrier to overcoming a negative or traumatic experience.[131] Erasure of sensitive personal information at the source aims to eliminate the audience. Even obscurity measures can reduce the size of the audience and in particular can help to reduce the incidence of connecting humiliating information with a person's name.[132]

---

128. *Ibid* at paras 70, 75-76. See also OPC, *Draft OPC Position*, *supra* note 4. OPC stresses this point as:

> [T]here 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 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 (*ibid*).

129. See generally Karine Nahon & Jeff Hemsley, *Going Viral* (Cambridge, UK: Polity Press, 2013).

130. Brian Leiter, "Cleaning Cyber-Cesspools: Google and Free Speech" in Saul Levmore & Martha C Nussbaum, eds, *The Offensive Internet: Speech, Privacy, and Reputation* (Cambridge, Mass: Harvard University Press, 2010) 155; Policy and Research Group of the Office of the Privacy Commissioner of Canada, *Online Reputation: What are they saying about me?* (Gatineau, Que: Office of the Privacy Commissioner of Canada, 2016) at 2; Nicolaus Mills, "Television and the Politics of Humiliation," *Dissent* 51:3 (July 2004) 79, online: <www.dissentmagazine.org/article/television-and-the-politics-of-humiliation>; See also Citron, *supra* note 116.

131. Martin, "Conceptualizing the Harms Done," *supra* note 121 at 269-71; Ganaele Langlois & Andrea Slane, "Economies of reputation: the case of revenge porn" (2017) 14:2 Comm & Crit/Cult Stud 120 [Langlois & Slane, "Economies of Reputation"]; Julia von Weiler, Annette Haardt-Becker & Simone Schulte, "Care and treatment of child victims of child pornographic exploitation (CPE) in Germany" (2010) 16:2 J Sexual Aggression 211 at 216-18.

132. Andrea Slane & Ganaele Langlois, "Debunking the Myth of 'Not My Bad': Sexual Images, Consent, and Online Host Responsibilities in Canada," 30:1 CJWL 42 [Slane & Langlois, "Debunking the Myth"]; Slane, "Information Brokers," *supra* note 40.

The mysterious nature of information processing in digital technology refers to the phenomenon of data mining, whereby companies (and governments) amass tremendous amounts of data regarding online activities that are or can be linked to a particular user. The secret nature of this processing—including what information has been collected and how it is being used—is also linked with the "surveillance society" effect.[133] It is a companion of the "attention economy" that creates value out of immaterial labour, using the actions of viewers to generate profit for companies who know how to direct the public's attention or turn people's viewing habits into valuable aggregated data about consumer behaviour.[134] The algorithms that produce search engine results are protected as trade secrets, a "black box" that is resistant to transparency and accountability.[135] For example, in *Google Spain*, it is not clear why a small newspaper announcement about an auction would turn up eleven years later in a search of Costeja González's name. It might have been related to the popularity of other items that were made available through the newspaper archive at the time or perhaps to the high relevance of Costeja González's name to the limited content of that short announcement. Google's closely guarded algorithm makes this guesswork.[136]

Finally, the uncontrollability of digital technology is related to various factors. Not only is there a lack of control in relation to big data, private individuals can also disseminate vast amounts of content, including content containing sensitive personal information of others, while facing few, if any, constraints. Social media, in particular, has led to two (sometimes toxic and interrelated) trends that are fostered by the easy ability to anonymize online postings and the historical reluctance of online platforms to interfere with user-generated content. First, social media encourages a logic of popularity and consumption (amassing "likes" and "re-tweets"). Second, it fosters online incivility, "trolling," and shaming.

133. David Lyon, "Surveillance, Snowden, and Big Data: Capacities, consequences, critique" (2014) 1:2 Big Data & Soc 1; See generally Bennett et al, *supra* note 24; Daniel Trottier, "Interpersonal Surveillance on Social Media" (2012) 37:2 Can J Comm 319.
134. Thomas H Davenport & John C Beck, *Attention Economy: Understanding the New Currency of Business* (Boston: Harvard Business School Press, 2001). For a critique, see Kenneth Rogers, *The Attention Complex: Media, Archeology, Method* (New York: Palgrave Macmillan, 2014).
135. Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, Mass: Harvard University Press, 2015).
136. *Ibid*; Engin Bozdag, "Bias in algorithmic filtering and personalization" (2013) 15:3 Ethics & Info Tech 209.

As an example of the "subculture of humiliation" phenomenon, social media actually rewards people for being mean in a catchy way.[137]

The presumed uncontrollability of user behaviour is an affordance and a choice, rather than a necessity. Technology companies that run the search engine platforms regularly distinguish themselves based on their formula for curating content, as well as their enabling of user expression.[138] It is clear now that claims like "information wants to be free" and "there is no privacy, get used to it," reflect a manufactured rather than a natural absence of control.[139] This tension is especially evident in the United States, where there is a preference for market solutions to private sector problems. Section 230 of the *Communications Decency Act* (*CDA*) enshrined immunity for intermediaries from many, though not all forms of legal regulation. The legislation's original aim was to encourage hosts and platforms to curate content to filter out objectionable material according to their users' preferences.[140] By design, the legislation prefers some forms of content to others: It preserves liability for intellectual property infringement, federal law, and some state criminal law, while deliberately eschewing others (for instance, there is no liability for civil actions that would require the intermediary to be deemed a "publisher" of third-party content).[141] Danielle Keats Citron notes that the immunity provided has sheltered businesses that capitalize on the worst impulses of human expression, expressly to facilitate "cyber cesspools."[142] Taken together, the outcomes of section 230 of the *CDA* demonstrate how political

---

137. One particularly noxious form of popular online humiliation is websites dedicated to "revenge porn," where users are encouraged to post sexual images of other people without their consent and other users are encouraged to comment on those photographs. See Langlois & Slane, "Economies of Reputation," *supra* note 131; Scott R Stroud, "The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn" (2014) 29:3 J Mass Media Ethics 168. Dedicated revenge porn websites can be considered a form of social media in that they are primarily dedicated to user-generated content, though similar dynamics of user posting and user commentary occur on more traditional social media platforms as well. See "Facebook warned over legal action after revenge porn case," *BBC News* (13 January 2018), online: <www.bbc.com/news/uk-northern-ireland-42675036>.
138. Grimmelmann, *supra* note 91 at 875.
139. Lawrence Lessig, *Code: And Other Laws of Cyberspace, Version 2.0* (New York: Basic Books, 2006) at 24. For an example of platforms claiming "there is no privacy, get used to it," see Polly Sprenger, "Sun on Privacy: 'Get Over It,'" *Wired* (26 January 1999), online: <www.wired.com/1999/01/sun-on-privacy-get-over-it>. See also Jack Goldsmith & Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (Oxford, UK: Oxford University Press, 2006).
140. Citron, *supra* note 116 at 170-71.
141. *Communications Decency Act*, 47 USC § 230 (1996) [*CDA*].
142. Citron, *supra* note 116 at 171-72.

choices about what information flows are or are not interfered with do not 'break the Internet'—it is the way Internet design has always operated, and alternative choices are available.[143]

The policy that intermediaries should not be liable for hosting or otherwise enabling third-party content is no doubt important to encourage the development of these services; otherwise, they would be unduly hampered by the burden of having to filter harmful content to avoid liability.[144] However, this does not mean that these services have no responsibility for their dealings with that content. Once the public availability of personal information has been determined to be harmful or, as in the EU, to violate a data subject's fundamental rights in ways that are not trumped by the rights of the content provider or the public to have access to that information, these services can and have been obligated to act in the data subject's interest.

Search engines are responsible for the specific type of information processing that involves harms or rights infringements arising from ranking information located elsewhere in a way that brings that information, especially the most highly ranked results, to the users' attention. When inappropriate information is highly ranked, this can be the result of a failure of the algorithm (which is perhaps what happened in Costeja González's case). Alternatively, the algorithm might be successful, but it fails to consider factors that might be crucial to appropriate information flow (*e.g.*, factors related to harm or risk of harm to subjects, as discussed above in Part II).[145] In that sense, when search engines like Google either voluntarily or by compulsion de-list or de-index content or manipulate search results for particular terms, they recognize that they have both the power and the responsibility to correct at least some of these failures or oversights.

As noted above in Part I(A), in *Equustek* Google argued that its "reporting to users the existence of publicly accessible websites" is speech that should be protected by the *Charter*, and that the users' speech rights are infringed whenever a law prevents them "from using Google's search engine to find and access

143. Jonathan Zittrain, *The Future of the Internet: And How to Stop It* (New Haven: Yale University Press, 2008).

144. There is a qualitative difference between imposing liability on intermediaries for hosting merely third-party content or for hyperlinking, and imposing responsibilities on businesses that collect, process, and package personal information for profit (*e.g.*, returning search results). For a discussion on hyperlinking and defamation liability, see *Crookes*, *supra* note 84 at para 42.

145. Gratton & Polentsky, *supra* note 13 at 18-24.

information that is publicly available on the Internet."[146] However, in addition to ignoring the fact that users routinely do not "find and access information that is publicly available on the Internet" (since Google already manipulates search results), this argument presumes that users have a right to access the links that Google would no longer suggest in its results, which is not necessarily the case. All Canadian regimes dealing with information flow—from the *Charter* to *PIPEDA* to access to information legislation[147]—consider access to personal information, especially sensitive personal information, to be justifiably subject to greater limitations than access to other forms of information. Information is considered sensitive when there is a high likelihood that its public release would cause the data subject harm.[148] The right to be forgotten—including as applied to search engines—can be implemented in the same spirit as these other access to information regimes, whereby the right to access is tempered by important competing values concerned with shielding data subjects from harm. While Google should certainly be sheltered by the concept of "innocent dissemination," it should also be required, in appropriate circumstances, to participate in achieving a better balance between the various values at stake in personal information flow.

III. INFORMATION FLOW OF PUBLIC DOCUMENTS IN CANADA

As should be evident by now, the most controversial aspects of the right to be forgotten arise from what is often characterized as the manipulation of access to publicly available information online. The controversy is fanned by the fact that in the United States, information that has gone public—even if illegally so—is often considered fair game for publication and republication.[149]

146. *Equustek* FOA, *supra* note 89 at para 27. The debate about the contours of "machine speech" is relevant in different ways in the United States and in Canada. This is because recognizing that search results are "speech" does not place insurmountable burdens on finding a balance with other values like privacy and identity rights in Canada. See Tim Wu, "Machine Speech" (2013) 161:6 U Pa L Rev 1495; Stuart Minor Benjamin, "Algorithms and Speech" (2013) 161:6 U Pa L Rev 1445; Eugene Volokh & Donald M Falk, "Google: First Amendment Protection for Search Engine Search Results" (2012) 8:4 JL Econ & Pol'y 883; Frank Pasquale, "Search as Speech: Two Scenarios" (29 May 2012), *Concurring Opinions* (blog), online: <concurringopinions.com/archives/2012/05/search-as-speech-two-scenarios.html>.

147. At the federal level, the legislation governing access to information is the *Access to Information Act*, RSC 1985, c A-1. All provinces have comparable access to information legislation addressing provincial and municipal governments.

148. Paul Ohm, "Sensitive Information" (2015) 88:5 S Cal L Rev 1125 at 1133.

149. *Cox Broadcasting Corp v Cohn*, 420 US 469 (1975) [*Cox Broadcasting*]; *Florida Star v BJF*, 491 US 524 (1989) [*Florida Star*]; *Smith v Daily Mail Pub Co*, 443 US 97 (1999) [*Daily Mail*].

Further, some material that is legally suppressed (*e.g.*, defamatory content) is allowed more leeway online than offline. The adaptation of the "single publication rule" to online contexts has ensured that despite the fact that information on the Internet is potentially 'forever,' the statute of limitations runs from the first time that material is published online.[150] Further, the *CDA* section 230 immunity has been held to apply even when the host of the defamatory content shares the publication incentives with the original speaker.[151] Of course, even in the United States, some online information flows can be legally suppressed (*e.g.*, child pornography, material that infringes copyright, and other illegal content). However, a larger swath of information cannot be legally suppressed once it is 'out there.'

Because Canada has approached the regulation of personal information flow in public forums differently than the United States, there are potentially different values to consider and different choices to make when weighing options regarding the right to be forgotten. Additionally, although Canadian jurisprudence on the freedom of expression rights of recipients of others' personal information is sparse, it leans towards deeming limitations on access of personal information to be justified. Most of the Canadian jurisprudence on listeners is about regulating content deemed to be generally harmful (*e.g.*, obscenity, hate speech, and manipulative commercial speech), where the value of the speech is reduced by its derogation from the autonomy of the listeners themselves due to its potentially manipulative character.[152] Defamation jurisprudence similarly affords speakers leeway to engage in "responsible communication on matters of public interest," in part because the "responsible" quality supports listener autonomy, enabling listeners to reasonably judge for themselves.[153] Privacy-invasive content has been treated differently. In the seminal SCC case *Aubry v Éditions Vice-Versa Inc,* which is rooted in Quebec's greater privacy protections, the Court considered the public's right to access expression (in this case, a photograph of the plaintiff published by the defendant magazine). The Court held that the rights of the photo subject to determine whether to consent to the publication outweighed the public's right to

150. Lori A Wood, "Cyber-Defamation and the Single Publication Rule" (2001) 81:4 BUL Rev 895; Sapna Kumar, "Website Libel and the Single Publication Rule" (2003) 70:2 U Chicago L Rev 639; Adeline A Allen, "Twibel Retweeted: Twitter Libel and the Single Publication Rule" (2014) 15:1 J High Tech L 63.

151. *Blumenthal v Drudge*, 992 F Supp 44 at 51-52 (DDC 1998). For critical discussion of this overly generous approach to *CDA* s 230 immunity, see Felix Wu, "Collateral Censorship and the Limits of Intermediary Immunity" (2011) 87:1 Notre Dame L Rev 293.

152. Richard Moon, "Justified Limits on Free Expression: The Collapse of the General Approach to Limits on *Charter* Rights" (2002) 40:3&4 Osgoode Hall LJ 337.

153. *Grant v Torstar Corp*, 2009 SCC 61 at paras 51-57, [2009] 3 SCR 640 [*Grant*].

see that photograph. In other words, the public's right to receive that expression was not strong enough to override the need to obtain consent, even though the photo did not contain particularly sensitive personal information.[154]

When exploring these choices, it will be useful to consider three categories of publicly available information: (a) material that should not have been made public in the first place, (b) material that is on the public record but to which access is justifiably restricted, and (c) material that has gained (or regained) greater prominence than it warrants because of the unpredictable way that information dynamics and the algorithms that mine this material work online.[155]

D. MATERIAL THAT SHOULD NOT HAVE BEEN MADE PUBLIC IN THE FIRST PLACE

Several categories of personal information are prohibited from being published in Canada, including non-consensual publication of intimate images,[156] voyeuristic

154. *Aubry v Éditions Vice-Versa Inc*, [1998] 1 SCR 591 at paras 57, 65, 157 DLR (4th) 577. Canada is also beginning to develop case law on privacy torts, including publication of private facts. In Ontario's first case that explicitly endorsed a tort of publication of private facts, the court adopted the US test that the publication of the material be highly offensive to a reasonable person and "not of legitimate concern to the public." See *Jane Doe 464533 v ND*, 2016 ONSC 541 at paras 46-47, 128 OR (3d) 352. In this case, publication of an intimate photograph shared with the defendant in confidence was deemed to be devoid of any legitimate public concern. This case involved a defendant who refused to defend himself, since he believed that there was no valid cause of action. The judgment has since been set aside in order to allow him to present a proper defence. See *Jane Doe 464533 v ND*, 2016 ONSC 4920, 276 ACWS (3d) 55; *Jane Doe 464533 v ND*, 2017 ONSC 127, 276 ACWS (3d) 261. While this leaves the original reasons regarding the availability of a tort of publication of private facts in limbo, it does not directly invalidate them as an indication of the willingness of Ontario courts to recognize this tort.

155. These classifications are similar to those proposed by the OPC as being among the circumstances where search engines could be required to de-list or de-index results, namely where the "content is unlawful, or unlawfully published" and "[w]here the accessibility of the information may cause significant harm 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." See OPC, *Draft OPC Position*, *supra* note 4.

156. *Criminal Code*, RSC 1985, c C-46, s 162.1(1) [*Criminal Code*]. Section 162.1(1) states:

> Everyone who knowingly publishes, distributes, transmits, sells, makes available or advertises an intimate image of a person knowing that the person depicted in the image did not give their consent to that conduct, or being reckless as to whether or not that person gave their consent to that conduct [commits an offence].

A public interest defence is also set out (*ibid*, s 162.1(3)).

images,[157] sensitive information that carries a high risk of identity theft (*e.g.*, financial identifiers, signatures, and account numbers),[158] and information held by trusted data custodians (*e.g.*, personal health information).[159] In general, publication of materials in these categories is considered to harm or risk harm to the data subject to a degree that outweighs the freedom of expression interests of the speakers and recipients. The Canadian government's consultation paper on voyeurism, for instance, rationalizes the creation of a criminal offence for the dissemination of images that qualify as voyeuristic, stating that "[t]he harm generated by criminal voyeurism is amplified when the visual representations are transmitted or distributed to other persons."[160] Search engines that facilitate user access to such harmful materials similarly amplify those harms.

The long process of creating the new offence of non-consensual distribution of intimate images, both in Canada and the United States, reflects the difficulties that persist in separating limited distribution from wider publication (here, allowing limited consensual sharing of sexual images, but punishing non-consensual wider dissemination of these images). Initially, the common response to victims' complaints was to blame them for their own misfortune, deploying the trope of uncontrollability noted above in Part II—*i.e.*, once an image exists, you no

157. *Ibid*, s 162(4). Section 162(4) states:

> Everyone commits an offence who, knowing that a recording was obtained by the commission of an offence under subsection (1), prints, copies, publishes, distributes, circulates, sells, advertises or makes available the recording, or has the recording in his or her possession for the purpose of printing, copying, publishing, distributing, circulating, selling or advertising it or making it available.

A public interest defence is also set out (*ibid*, s 162(6)).

158. *Ibid*, s 402.2(2). Section 402.2(2) states:

> Everyone commits an offence who transmits, makes available, distributes, sells or offers for sale another person's identity information, or has it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence.

159. Provincial offences address this issue. See *e.g. Personal Health Information Protection Act, 2004*, SO 2004, c 3, Sch A, s 72. This Ontario legislation makes it an offence to collect, use, or disclose personal health information. Penalties are fines up to $100,000 for a natural person and up to $500,000 for a non-natural person (*ibid*, s 72(2)).

160. Department of Justice Canada, *Voyeurism as a Criminal Offence: A Consultation Paper* (Ottawa: Department of Justice, 2002) at 11, online: <www.justice.gc.ca/eng/cons/voy/index.html>. As social media technology evolves, further adjustments to the balance between freedom of expression and privacy in public continue. See *e.g.* Robson Fletcher, "Social media 'creep' accounts flourish at the murky intersection of privacy rights and free speech," *CBC News* (16 June 2017) online: <www.cbc.ca/news/canada/calgary/canadacreep-laws-public-photography-voyeurism-1.4160436>.

longer have control over it, nor are you entitled to, so do not take sexual photos to begin with.[161] As noted above in Part II, the notion of irretrievable loss of control can have devastating consequences on a subject's mental health. The inherent popularity of pornography, combined with the subculture of humiliation, has led many women who are portrayed in such images to fear permanent and widespread destruction of their online identities.[162] In these instances, the right to be forgotten in the form of erasure from the source sites—and de-indexing from search engines when the hosts refuse to comply—provides an important remedy. Since 2015, most search engines and social media platforms have declared their voluntary policy to take down such images upon request by the subject.[163] The right to be forgotten would therefore need to be applied only when a search engine or another platform has refused to remove the images.

Material that is prohibited from publication should already be required to be deleted at the source, because knowingly hosting such material online should be considered dissemination.[164] Where the host is a true intermediary and does not monitor the content posted by users, this liability applies (as it does with most criminal offences) only when the host gains knowledge of its part in disseminating that material.[165] Similarly, search engines should be required to de-index sites that contain such information where hosts have not complied with their obligation to take the material down. Because this category of information has already been considered in relation to countervailing expression interests,

---

161. Langlois & Slane, "Economies of Reputation," *supra* note 131 at 124-25; Danielle Keats Citron & Mary Anne Franks, "Criminalizing Revenge Porn" (2014) 49:2 Wake Forest L Rev 345 at 348, 354.
162. Langlois & Slane, "Economies of Reputation," *supra* note 131 at 126; Samantha Bates, "Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors" (2017) 12:1 Fem Criminology 22 at 23; Amanda Lenhart, Michele Ybarra & Myeshia Price-Feeney, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn"* (New York: Data & Society Research Institute & Centre for Innovative Public Health Research, 2016) at 4.
163. Amit Singhal, "'Revenge Porn' and Search" (19 June 2015), *Google Public Policy Blog* (blog), online: <www.googlepublicpolicy.blogspot.com/2015/06/revenge-porn-and-search.html>; Techworld Staff, "Reddit to crack down on mean feeds" (17 July 2015), *Techworld* (blog), online: <www.techworld.com/news/apps/reddit-to-crack-down-on-objectionable-content-3620006>.
164. In the United States, even blatant "revenge porn" hosts have taken shelter behind s 230 of the *CDA*. See *CDA*, *supra* note 141. I have argued elsewhere that revenge porn hosts in Canada should not be protected from liability where their business model expressly encourages this grave form of privacy violation. See Slane & Langlois, "Debunking the Myth," *supra* note 132.
165. Knowledge and control are the component parts of possession at law, such as for the offence of possession of property obtained by crime. See *Criminal Code*, *supra* note 156, s 354(1).

requiring the assistance of intermediaries and search engines that generally (or specifically) profit from information dissemination merely acknowledges their role in both the problem and its solution.[166]

Defamation, as another category of information in which further publication is prohibited,[167] is stickier. Canadian law is still revising what counts as defamatory, what defences are available, and who is a publisher.[168] Recent revisions indicate that the freedom of expression interests are stronger here than in the above categories of materials for which dissemination is categorically prohibited. Enlisting the help of intermediaries and search engines to suppress defamatory material should continue to require a court order on a case-by-case basis. Following *Equustek*, judges would need to determine whether enlisting the assistance of search engines or other service providers is appropriate and specify what form that assistance should take (*e.g.*, de-listing, de-indexing, or erasure).

In other words, the right to be forgotten can in many cases be unproblematically applied in cases involving materials where publication or republication is already prohibited. This is because freedom of expression interests have been considered and limits on the public's right to access this information have been justified in favour of the data subject's dignity-based privacy and identity interests.

E. MATERIAL THAT IS PUBLIC BUT WITH JUSTIFIABLE ACCESS RESTRICTIONS

The second category of publicly available information involves material that is on the public record, but for which Canadian law or policy has implemented access restrictions to honour competing values.[169] These materials can be divided into two subcategories. The first includes materials that have been traditionally subject to the right to oblivion in Europe, based on the value of allowing a person to no longer be judged by past mistakes ("clean slate"). The second subcategory includes materials containing personal information that are available to the public to honour the "open court" principle. These materials are limited by access and publication restrictions to help shield the privacy of some of the people involved in a case.

---

166. See *Equustek*, *supra* note 84 at paras 31, 35, 73. The SCC reviews the case law supporting the capacity of Canadian courts to issue court orders compelling non-parties to assist plaintiffs in enforcing their rights where the non-party facilitates the wrongdoing of a defendant.
167. Publication to a third party is a component of the tort of defamation. See *Grant*, *supra* note 153 at para 28.
168. *WIC Radio Ltd v Simpson*, 2008 SCC 40, [2008] 2 SCR 420; *Grant*, *supra* note 153; *Crookes*, *supra* note 84.
169. Slane, "Information Brokers," *supra* note 40.

With regard to the "clean slate" category, Canada, like many other jurisdictions, has well-developed and long-acknowledged justifications for disallowing a person's past mistakes from following them forever in certain well-delineated circumstances. Pardons, restrictions on disclosure and use of juvenile criminal records, as well as bankruptcies and credit information all follow variants of the "clean slate" policies, for the good of both individuals and society as a whole.

Pardons, or record suspensions as we now call them in Canada, fulfill important policy objectives, including reducing crime.[170] When the federal government was amending the *Criminal Records Act*[171] in 2012, all members of the Standing Senate Committee agreed that the record suspension system is important and valuable.[172] Studies have proven that having criminal history information no longer appear on standard criminal record checks will assist in an individual's long-term rehabilitation and reintegration, significantly improve the person's overall prospects (health, financial, and family relationships), and reduce the likelihood of re-offending.[173] This effect in turn benefits the public because a person granted a record suspension is far more likely to find gainful employment and other social stability, and thus the individual would be less likely to become re-entangled with the criminal justice system, require social assistance, or suffer from substance abuse or other serious mental health issues.[174]

The impetus for the 2012 amendments to the *Criminal Records Act* was the Conservative federal government's argument that the system for record suspensions was too automatic. To be granted a record suspension, even for egregious crimes, a person had to have stayed out of trouble merely for the required number of years after serving their sentence. The amendments introduced additional factors that the Parole Board could consider, including most significantly whether granting a record suspension would bring the administration of justice into disrepute. In other words, the amendments sought to deny record suspensions for morally 'unforgiveable' crimes, both categorical (*e.g.*, sexual crimes against children)

---

170. Rick Ruddell & L Tom Winfree, "Setting Aside Criminal Convictions in Canada: A Successful Approach to Offender Reintegration" (2006) 86:4 Prison J 452.
171. *Criminal Records Act*, RSC 1985, c C-47.
172. Senate of Canada, The Standing Senate Committee on Legal and Constitutional Affairs, *Bill C-23A, an Act to amend the Criminal Records Act and to make consequential amendments to other acts* (22 June 2010) (Chair: Joan Fraser), online: <www.parl.gc.ca/Content/SEN/Committee/403/lega/48300-e.htm>.
173. *Ibid* at Testimony: Harvey Cenaiko; Frank Pasquale, "Reforming the Law of Reputation" (2016) 47:2 Loy U Chicago LJ 515 at 535 [Pasquale, "Reforming the Law of Reputation"].
174. Senate of Canada, *supra* note 172 at Testimony: Heidi Illingworth.

and individual (*e.g.*, the serial killer Karla Homolka). After these amendments became law, the system now issues record suspensions for cases where 'forgiving' a person's crime—or more accurately, obscuring it from public knowledge by suppressing his or her record from standard criminal record checks—does not offend normative moral sensibilities.[175]

The criminal records of a person granted a record suspension are not erased. They are suppressed in the Canadian Police Information Centre ("CPIC") database and can be revived if the person commits a further offence. If other online information about that individual is limited and if the arrest or conviction was reported in a news source, it is certainly possible that the conviction will turn up in search results of that person's name, long after the sentence or resolution is completed. Our freedom of expression values may militate against subjecting news sources to erasure and by extension would not tolerate de-indexing news sites that house historical articles. However, the option of de-linking a reference to a person's past convictions in his or her name search upon the granting of his or her record suspension would be appropriate to fulfill the other important policy goals noted above in this Subpart. As with the criminal record, the historical record is preserved and is simply less automatically linked to current searches for information about that individual. This is in effect what the CJEU decided in *Google Spain*, and that approach would fit well within the Canadian record suspensions regime.

Credit and bankruptcy information is more complicated. Canada, like many jurisdictions, limits the amount of time that negative financial information can be used to assess the creditworthiness of a consumer.[176] However, with big data processing numerous data sources, the algorithms that assess creditworthiness by mining and aggregating public online information are even more mysterious than search results from a search engine. As Frank Pasquale pointed out, the removal of bankruptcy information from credit reports is undermined if that information continues to influence "lead generators' or social networks'

---

175. *Ibid* at Testimony: Honourable Vic Toews. Similarly, we suppress records of a juvenile offender (in addition to issuing publication bans and otherwise limiting access to juvenile criminal conviction records) on the belief that a young person has far better prospects of turning his or her life around and living a productive life if these events can be put behind an informational barrier. See Canada, Department of Justice, "Youth Records," online: <www.justice.gc.ca/eng/cj-jp/yj-jj/tools-outils/sheets-feuillets/recor-dossi.html> (referring to the *Youth Criminal Justice Act*, SC 2002, c 1 [*YCJA*]).

176. See *Consumer Reporting Act*, RSO 1990, c C.33, s 9(3). Section 9(3) sets out information not to be included in a credit report. The time limit for relevant financial information is generally seven years (*ibid*).

assessments of creditworthiness, and would-be lenders are in some way privy to those or similar reputational reports."[177] He noted that these types of background data processing, like the formulas that yield search results, are "automated, algorithmic arrangements of information, which could render a data point removed or obscured in one records system, and highly visible or dominant in other, more important ones."[178] For credit information, the "clean slate" policy regarding outdated information can be enforced only when consumers know what information is contained in their digital dossier—as they would if some of that information turned up in search results of their name—and have a means to object to further processing.

As with protected yet public information, a bankruptcy that was reported in a public news source does not need to be erased at its source. Instead, as in *Google Spain*, outdated financial information that has been publicly reported needs to be subjected to an analysis of public interest to determine whether de-listing the reference to that news source upon a search of the data subject's name is appropriate. Alternatively, the search engine's algorithm could be tweaked to adjust the ranking of such information. This would in effect demote the information rather than de-link it as it ages.[179] As with criminal records, if further financial troubles plague the data subject, the relevance of past financial troubles would increase again. Multiple bankruptcies are certainly relevant to an individual wanting to do business with a data subject; therefore, easier access to this information would be in the public interest.

The main countervailing interest for the second category of public records to which Canadian law or policy justifiably limits access is the value of open courts—that public observation can ensure justice is properly served. Restrictions on publication have been discussed in two main arenas: the extensive Canadian jurisprudence on publication bans and the more recent discussions of online court decision databases, as in the case of *Globe24h*.

Publication bans differ greatly between Canada and the United States. Canada allows publication bans based on privacy and identity interests for victims of sexual assault, as well as for juvenile offenders, their victims, and any witnesses in juvenile criminal proceedings. Additionally, publication bans in Canada are mandatory for information that could identify complainants or witnesses in sexual assault trials upon the request of the complainant, witness, or prosecutor.[180]

---

177. Pasquale, "Reforming the Law of Reputation," *supra* note 173 at 516.
178. *Ibid*.
179. Powles, *supra* note 3 at 599; Ambrose, *supra* note 10.
180. *Criminal Code*, *supra* note 156, s 486.4(1)-(2).

Judges can decide to issue such an order even without a request.[181] Judges can also impose publication bans on information that can identify any victim of crime who is under eighteen.[182] Publication of the identity of a young person who is an accused, victim, or witness in a youth justice matter is automatically prohibited.[183] Although members of the public are generally permitted to attend any of these hearings and view (but not photocopy) court documents, the fact that the person's identity is available to the public in the courtroom and in documents housed at the court does not preclude a prohibition on broader public dissemination. These publication bans are considered a justifiable restriction on freedom of expression that protects the privacy and identity interests of the people concerned. They help to shield young offenders from the stigma that serves as a barrier to rehabilitation, encourage victims to report sensitive crimes, and encourage witnesses to participate in the justice process, while at the same time valuing the transparency and accountability supported by the open court principle.

The United States takes a very different approach to publication bans and the responsibilities of publishers. Several United States Supreme Court rulings have confirmed that once information has been released, even illegally, its further publication cannot be prohibited without falling afoul of the First Amendment.[184] Parties must make applications to the court or avail themselves of standing court policies to protect identity interests, *e.g.*, to keep names and images of sexual assault victims out of public records, close the courtroom during witness testimony, grant alternative methods to provide testimony (such as by video), or seal records.[185] In other words, the responsibility for protecting a person's identity lies entirely with the government; publishers have no legal obligation to do so. Mainstream news outlets usually have ethical guidelines about identifying victims. However, one study found that more than 50 per cent of news articles about child victims of sexual or other abuse included identifying information,

181. *Ibid*, s 486.5(1).
182. *Ibid*, s 486.4(2.1).
183. *YCJA*, *supra* 173, s 110. The ban can be lifted if the young person is given an adult sentence, or if a judge determines it is in the public interest to disclose his or her identity in relation to having committed a violent crime.
184. *Cox Broadcasting*, *supra* note 149; *Florida Star*, *supra* note 149; *Daily Mail*, *supra* note 149.
185. National Crime Victim Law Institute, *Confidentiality and Sexual Violence Survivors: A Toolkit for State Coalitions* (Portland: NCVLI, 2005).

despite research that strongly suggests that publicity is highly detrimental to the recovery of these victims.[186]

Canada can therefore enforce publication bans on online publishers in ways that are unavailable in the United States. Intermediaries and information location services like search engines can be enlisted to enforce publication bans meaningfully: Upon notice, any host or search engine could be required to delete or de-index a source that violates a publication ban. The balancing of freedom of expression interests with protecting privacy, identity, and the administration of justice has already been carried out in issuing the publication ban (which can, of course, be challenged in itself). Therefore, hosting further publications or making this material easy to find does not revive new freedom of expression interests that have not already been considered in granting the application for the ban.

The second arena for protecting the privacy and identity interest of people whose names and other personal information appear in public court documents involves online court decision databases.[187] These databases have policies that do not allow their sites to be collectively indexed by search engines (*i.e.*, each site has its own internal search tool). In *Globe24h*, the website republished Canadian court decisions and allowed them to be indexed by search engines, while charging a fee to individuals who wanted to have their documents removed from the site, as well as generating revenue from advertising.[188] The OPC and in turn the Federal Court rejected Globe24h's claim that it fell within the "journalistic purpose" exception to the application of *PIPEDA*, as well as the "publicly available documents" exception to the requirement to obtain the data subject's consent.[189]

---

186. Lisa M Jones, David Finkelhor & Jessica Beckwith, "Protecting victims' identities in press coverage of child victimization" (2010) 11:3 Journalism 347 at 353.
187. See generally Office of the Privacy Commissioner of Canada, *Electronic Disclosure of Personal Information in the Decisions of Administrative Tribunals* (Guidance Document) (Ottawa: Office of the Privacy Commissioner of Canada, 2010), online: <www.priv.gc.ca/media/4082/gd_trib_201002_e.pdf> [OPC, *Electronic Disclosure*]; Canadian Judicial Council – Judges Technology Advisory Committee, *Model Policy for Access to Court Records in Canada* (Ottawa: Canadian Judicial Council, 2005), online: <www.cjc-ccm.gc.ca/cmslib/general/news_pub_techissues_AccessPolicy_2005_en.pdf> [CJC, *Model Policy*].
188. Office of the Privacy Commissioner of Canada, *Website that generates revenue by republishing Canadian court decisions and allowing them to be indexed by search engines contravened PIPEDA*, PIPEDA Report of Findings #2015-002 (Ottawa: Office of the Privacy Commissioner of Canada, 5 June 2015), online <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-002>.
189. *Ibid* at para 68.

In evaluating the defendant's claim to shelter under the "publicly available documents" exception to the requirement to secure consent, the Federal Court endorsed the OPC's reasoning that court and tribunal websites, as well as free legal databases like CanLII and SOQUIJ, do not allow their sites to be indexed by search engines. The main reason for this restriction is that "in spite of the importance of individuals' electronic access to judgments, that a restriction against web indexing is necessary to address a serious risk to individual privacy, and that the benefits of such a restriction outweigh the negative impacts on the open courts principle."[190] The OPC and in turn the Federal Court concluded that inadvertently finding court decisions through searches of a person's name on a general search engine does not further the open court principle, and so it does not comport with the purpose for making these decisions available to the public in the first place.[191] The Federal Court thus issued the order that would allow the complainant to appeal to Google to de-list the site.[192]

A complicating fact in the circumstances of this case is that in the meantime, Globe24h has discontinued its practice of charging fees to remove individual documents from the site and appears to have ceased to solicit advertising. If the website is no longer a commercial venture, it may not be subject to *PIPEDA* obligations in Canada anymore, since the data protection legislation only applies to organizations engaged in commercial activities.[193] This development speaks to the need to apply *PIPEDA* to Google directly, since Google remains a commercial venture that would otherwise continue to provide links to a newly non-commercial variant of Globe24h; despite the fact that Globe24h allows indexing of court decisions and documents for profit or not, the reasoning regarding balancing of privacy, consent, and the open court principle remains the same.[194]

In principle, the Canadian practice of making court decisions public but not endorsing indexing by search engines would be easily achieved by requiring

---

190. *Ibid* at para 85. See also OPC, *Electronic Disclosure*, *supra* note 187; CJC, *Model Policy*, *supra* note 187.
191. *Globe24h*, *supra* note 5 at paras 75-76. The Federal Court characterized the allowance of general search engines to index court documents as "needless exposure of sensitive personal information of participants in the justice system" (*ibid* at para 76).
192. *Ibid* at paras 80-96.
193. *PIPEDA*, *supra* note 4, s 4.
194. Mark Hayes and Adam Jacobs comment that *Globe24h* makes an "unnecessary detour" into the "appropriate purpose" section of *PIPEDA*, when the case could have been resolved exclusively via the consent requirement. This is a related point to the discussion, though it does not tackle the problem of the application of *PIPEDA* to a website or another service that is not commercial. See Mark Hayes & Adam Jacobs, "Forget the 'right to be forgotten' until the right case comes" (24 March 2017) 36:43 Lawyers Weekly (QL).

search engines to de-index sites that offer Canadian court documents. This would result in a site like Globe24h having to merely follow the same rules that other public online court decision databases already voluntarily follow.[195]

F. MATERIAL THAT IS INAPPROPRIATELY PROMINENT DUE TO THE OPERATION OF DYNAMIC SEARCH ALGORITHMS

The third category of publicly accessible material that has been targeted by the EU's right to be forgotten is any information pertaining to a data subject that he or she objects to being online. Boldly stated like this, this category takes further the principle that data subjects must consent to the public dissemination of their personal information, and on its face seems to trample unjustifiably on freedom of expression when applied to search engines. Nonetheless, with proper justification, an avenue should be explored for redressing instances when the search engine's algorithms have given undue and harmful prominence to sensitive personal information. As the OPC puts it, these are circumstances when either no public interest exists in access to that information via a name search or "the harm, considering its magnitude and likelihood of occurrence, outweighs any public interest."[196]

The role and functions of search engine algorithms in bringing material to public prominence can offer some guidance about when intervention might be appropriate. For example, old or minor information is far more likely to be prominently displayed on a name search of a person who does not have a very substantial online presence, compared to a person who has an active and robust online presence. Humiliating personal information may rise to the top of the list of a name search of an individual if it is popular, especially if that person does not have other significant online content associated with them.[197] In some cases, like Costeja González's in *Google Spain*, the prominence of a particular result is hard to explain. In each of these scenarios, the algorithm specifically

195. *Globe24h*, *supra* note 5 at paras 74, 99. See also Office of the Privacy Commissioner of Canada, *Online legal database doesn't need consent to use publicly available court decisions, in support of the open court principle*, PIPEDA Report of Findings #2015-013 (Ottawa: Office of the Privacy Commissioner, 21 September 2015), online <www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-013>.

196. OPC, *Draft OPC Position*, *supra* note 4.

197. Mary Anne Franks, "Unwilling Avatars: Idealism And Discrimination In Cyberspace" (2011) 20:2 Colum J Gender & L 224 at 256; Ann Bartow, "Internet Defamation as Profit Center: The Monetization Of Online Harassment" (2009) 32:2 Harv JL & Gender 383 at 429; Allison Woodruff, "Necessary, Unpleasant, and Disempowering; Reputation Management in the Internet Age" in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Toronto: CHI, 2014) 149, online: <dx.doi.org/10.1145/2556288.2557126>.

harms an individual's online identity interests either through its failure to return current and relevant results or, even if it yielded successful search results, its failure to account for the distorting impact of a data subject's low online prominence relative to the popularity of sites dedicated to public humiliation.[198] If outdated information unreasonably appears prominently in the search results of a data subject's name, granting a right to obscurity could be justified to compel correction of such skewed results.[199]

As Google works through the thousands of de-listing and de-indexing requests it continues to receive from European data subjects after *Google Spain*, it must be developing ways to weigh the factors involved in determining whether its algorithm is inappropriately promoting content.[200] Google reports that the most common requests to de-link content pertain to social media and other user-generated content. The search engine recognizes that much of this content is especially sensitive and damaging but is not of significant public interest; therefore, this factor tips the balance of freedom of expression in favour of the data subject's identity and privacy rights.[201] However, Google has not been forthcoming about the nature of the content pertaining to social media sites in these data subject requests. In order to ensure that an appropriate balance is struck between freedom of expression and privacy, Google's decision-making processes should be subject to a confidential audit by a neutral authority with expertise in both data protection and freedom of expression.

Although such an authority currently does not exist in Canada, the OPC suggests that it could potentially fill this role. The OPC further suggests, however, that Parliament also study the issue of how an appropriate balance between data

198. The prominence of negative information in search results is especially acute in relation to websites that promote the public accessibility of mugshot photographs. Barry Schwartz discusses how Google recently altered its algorithm to demote websites that compiled publicly available mugshots for the purposes of entertaining users and, in doing so, humiliated the data subjects. See Barry Schwartz, "Google Launches Fix to Stop Mugshot Sites from Ranking: Google's MugShot Algorithm" (7 October 2013), *Search Engine Land* (blog), online: <searchengineland.com/google-launches-fix-to-stop-mugshot-sites-from-ranking-googles-mugshot-algorithm-173672>. Jane E Bobet discusses the harm caused by publicly available mugshots more generally. See Jane E Bobet, "Mug Shots and the FOIA: Weighing the Public's Interest in Disclosure Against the Individual's Right to Privacy" (2004) 99:3 Cornell L Rev 633 at 634-35.

199. Ambrose, *supra* note 10.

200. Google, "Transparency Report," *supra* note 79.

201. Gratton and Polonetsky engage in a useful discussion of the meaning of "public interest" in Canadian law. For instance, the authors argue that mere curiosity or prurient interest is not enough to qualify as publication in the "public interest." See Gratton & Polonetsky, *supra* note 13 at 35.

protection principles and freedom of expression could best be achieved.[202] The emerging principles for determining when and when not to de-list suggest that it is possible for the government to develop concrete guidelines for de-listing and de-indexing search results that address some of the more egregious problems, while still respecting the freedom of expression. However, the question is, who would enforce those guidelines when they are not followed?

Many scholars have been wary of granting private companies like Google all of the decision-making power in dealing with requests from data subjects to have links removed.[203] Google prefers this, as all private companies do, over government regulation. The OPC however sees imposing data protection obligations on search engines to be in keeping with *PIPEDA* imposing its requirements on private companies who are personal information custodians.[204] In this sense, the process established in the wake of *Google Spain* is a working compromise in that Google makes decisions to list or de-list, and requesters can appeal to data protection authorities and ultimately courts when they disagree with a search engine's decision.[205] However, the avenue for content providers to appeal these decisions is less clear. A Canadian variant of this process should be simplified in parallel to the data subject's complaints process.[206] Avenues for complaints regarding user expression rights currently do not exist, though Google (and the OPC) are currently considering factors that appear to bear these avenues in mind.

A creative solution may be necessary to resolve these complex issues: A neutral arbiter could be created to deal with complaints about online content removal, including de-listing and de-indexing. The arbiter can balance the interests of all four categories of stakeholders (*i.e.*, service providers, data subjects, content providers, and users) and ensure that both data protection principles and

---

202. OPC, *Draft OPC Position*, *supra* note 4.
203. *Powles*, *supra* note 3 at 599; Jones, *supra* note 23 at 178-79; Gratton & Polonetsky, *supra* note 13 at 43. For an argument for the role of neutral arbiters more generally, see Pierre Trudel, "La responsabilité sur internet en droit civil québécois" (Report delivered at Le Colloque de Droit Civil 2008 de L'institut National de la Magistrature, Ottawa, 13 June 2008) at 1, online: <www.pierretrudel.net/files/sites/6/2015/01/TRUDEL_resp_internet.pdf>.
204. OPC, *Draft OPC Position*, *supra* note 4.
205. *Google FAQs*, *supra* note 74 at FAQ: "What happens if an individual disagrees with your decision?".
206. Google notifies webmasters of URLs that are de-listed but does not name the individual requesting the de-listing to protect that person's privacy as well as the integrity of the process. Google states that webmasters who receive such a notice through its "Webmaster Tools" can request a re-review of the decision. See *ibid* at FAQ: "Do webmasters have any way of challenging your decisions?".

freedom of expression are appropriately honoured. This solution could continue to rely largely on the voluntary compliance of search engines (and potentially social media platforms) in a "co-regulatory" model—a kind of private-public partnership for adjudicating complaints.

A version of this type of co-regulatory approach—albeit with less teeth than EU data protection authorities following *Google Spain*—is the Office of the eSafety Commissioner recently established in Australia.[207] The eSafety Commissioner administers a complaints system addressing a variety of complaints about online content, especially pertaining to serious online bullying of Australian children, through the voluntary compliance of social media platforms, combined with the eSafety Commissioner's power to broker solutions with uncooperative services and its capacity to appeal decisions to courts when a satisfactory resolution is not reached. The Office of the eSafety Commissioner has also assumed the responsibilities for handling complaints about illegal online content (mainly child pornography), statutorily allocated to the Australian Communications and Media Authority ("ACMA"). The ACMA staff continues to support the eSafety Commissioner in performing some of its mandate, although the Office of the eSafety Commissioner operates as a separate, independent entity.[208]

Like the eSafety Commissioner, a similar co-regulatory regime for complaints about online content removal, which includes de-listing and de-indexing, could be created in Canada, either as a wholly new entity or as an independent office within the OPC. The office could issue guidelines, like those suggested

---

207. The Office of the eSafety Commissioner was established by legislation in 2015 as the Office of the Children's e-Safety Commissioner in order to address complaints about cyberbullying of young Australians. The mandate was expanded to promote online safety for all Australians in 2017. See *Enhancing Online Safety Act 2015* (Cth); *Enhancing Online Safety for Children Amendment Act 2017* (Cth). The Office of the eSafety Commissioner "co-ordinates and leads the online safety efforts of government, industry and the not-for-profit community." In addition to serving as a complaints adjudication service for young Australians experiencing "serious cyberbullying," the Office of the eSafety Commissioner now also serves the function of identifying and removing illegal online content, including image-based abuse (non-consensual pornography). See Office of the eSafety Commissioner, "Role of the Office," online: <www.esafety.gov.au/about-the-office/role-of-the-office>. Some Australian legal scholars argue for further expansion of the Office of the eSafety Commissioner's mandate, endorsing the appropriateness of this co-regulatory model for dealing with issues like non-consensual pornography and online racism. See Nicolas Suzor, Bryony Seignior & Jennifer Singleton, "Non-Consensual Porn and the Responsibilities of Online Intermediaries" (2017) 40:3 Melbourne UL Rev 1057 at 1088; Gail Mason & Natalie Czapski, "Regulating Cyber-Racism" (2017) 41:1 Melbourne UL Rev 284 at 338.

208. Mason & Czapski, *supra* note 207 at 308-310; Office of the eSafety Commissioner, "About the Office: Legislation," online: <www.esafety.gov.au/about-the-office/legislation>.

in this article, for appropriate de-listing, de-indexing, and erasure of personal information of Canadian data subjects. The office could further conduct audits of decision-making processes and could administer complaints where requesters, content providers, or users are not satisfied with the result. Courts could then serve as the next layer of enforcement when warranted, just as they do currently with *PIPEDA* complaints.

Canadian courts' power to issue de-indexing orders to search engines, including the global or national reach of such orders, was dealt with by the SCC in *Equustek*.[209] As the OPC proposes, a more moderate solution than the worldwide order at issue in *Equustek* is the option for the courts to order search engines to employ geo-fencing technologies to de-list or de-index content despite the fact that only for people searching from within Canada, as Google currently does for its European privacy requests.[210] This geographically limited solution would still provide significant relief for most Canadian data subjects looking to reduce the impact of negative personal information online, because it would reduce the likelihood of people close to home viewing that material.

IV. CONCLUSION

Over the last twenty years, great innovations in digital information production and sharing have revolutionized what we know about each other and how. Initially, it was important not to interfere with the development of these platforms and services, which are now so thoroughly integrated into our social, professional, and personal lives. However, as our ability to harvest, package, and present information has matured, so too must our ability to adjust the matrices through which private entities process our information.

Search engines will play a central role in this adjustment because they influence how most people locate or are exposed to information about others. We know that search engines (and social media platforms) use mysterious algorithms to highlight certain materials over others. This does not mean that search engines and other hosts would become liable for third-party supplied content. Instead, privately owned search engines should be required to honour legitimate requests to de-link or de-index material that falls into the three categories described above in Part III.

---

209. *Equustek*, *supra* note 84 at para 41.

210. Samuel Gibbs, "Google to extend 'right to be forgotten' to all its domains accessed in EU," *The Guardian* (11 February 2016), online: <www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googlecom>; OPC, *Draft OPC Position*, *supra* note 4.

As Canada considers whether some version of the right to be forgotten can respect the Canadian values of privacy, access to information rights, and freedom of expression, it is important to consider the consequences of categorically denying that businesses that collect, process, and package publicly accessible information should be subject to data protection constraints. When protecting our 'privacy in public' from various forms of public and private sector surveillance, it is important not to categorically deny that public information collection and processing should be subject to regulation, even though that regulation will necessarily look somewhat different than the current data protection regime imposed on private sector actors who collect information directly from their customers.

Ultimately, the right to be forgotten, as with all regulation of Internet content and activity, is not an either-or, all-or-nothing kind of solution. Canadian law and policy regarding information flow has already established a legacy of balancing important values and interests. The right to be forgotten is an opportunity to bring that legacy to bear on digital technology in our current information environment, now and going forward.