

Canadian Law and the “Right to Be Forgotten”



innovation



results



value



gowlings

Lawyers • Patent and Trade-mark Agents

Canadian Law and the Right to Be Forgotten

- In Europe, the “Right to Be Forgotten” is synonymous with the *Google Spain v AEPD and González* decision and focuses on the ability to have search results delinked from the names of individuals when those results are “inaccurate, inadequate, irrelevant or excessive”
- The law in Canada today does **not** provide a foundation for this concept of the “Right to Be Forgotten”
- Canadian law **does** give individuals a degree of control over their personal information and protects against intentional misuses of that information. However, this is not the “Right to Be Forgotten” as it has come to be understood in Europe. The focus is not on search result delisting but rather on content publishers and other individuals/companies who deliberately and unlawfully misuse personal information

The Legal Foundation of *Google Spain v. AEPD and González*

- the *González* decision was based on an expansive interpretation of the European Union's Directive 95/46/EC (the 1995 Data Protection Directive)
- the 1995 Data Protection Directive is applicable to the “processing of personal data” by a “controller”

The Legal Foundation of *Google Spain v. AEPD and González*

- “processing”: any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use or disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction

The Legal Foundation of *Google Spain v. AEPD and González*

- “controller”: the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or community law

The Legal Foundation of *Google Spain v. AEPD and González*

- Article 6 specifies that a “controller” must take every reasonable step to ensure that data which does not meet the requirements under the Directive is erased or rectified.

Under the Directive:

- data must be adequate, relevant and not excessive in relation to the purposes for which it is collected and/or further processed
- accurate and kept up to date and kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed

The Legal Foundation of *Google Spain v. AEPD and González*

- Article 12(b) provides that Member States shall guarantee every data subject the right to obtain from the controller: ...
 - (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
- Article 14 provides the data subject with a general right to object to data processing

The Legal Foundation of *Google Spain v. AEPD and González*

- The Court of Justice of the European Union (CJEU) held that search engines are responsible for “processing” information within the meaning of the Directive, that they are “controllers” within the meaning of the Directive, and that in order to comply with the Directive:
 - “the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful”

Canada's Personal Information Protection and Electronic Documents Act

- PIPEDA and the substantially similar provincial legislation are not based on data processing by data controllers but rather establish rules to govern the collection, use and disclosure of personal information by organizations in the course of commercial activity
- In PIPEDA, commercial activity is defined to include:
 - any particular transaction, act or conduct or any regular course of conduct that is of a **commercial character**, including the selling, bartering or leasing of donor, membership or other fundraising lists.
- The courts have determined that just because a business engages in commercial activity, this does not mean that all of its activities with respect to personal information are of a commercial character and therefore subject to PIPEDA, see *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*

Canada's Personal Information Protection and Electronic Documents Act

- PIPEDA excludes from its scope:
 - (b) any individual in respect of personal information that the individual collects, uses or discloses for personal or domestic purposes and does not collect, use or disclose for any other purpose; or
 - (c) any organization in respect of personal information that the organization collects, uses or discloses for journalistic, artistic or literary purposes and does not collect, use or disclose for any other purpose.
- If PIPEDA were interpreted to give a broad right to seek delisting of search results, this would bypass or evade PIPEDA's existing limitations

Canada's Personal Information Protection and Electronic Documents Act

- The provisions of PIPEDA and similar laws are directed at the deliberate collection/use/disclosure of personal information in order to conduct business activities. This is apparent from the wording and structure of the laws and the key obligations, e.g.
 - Organizations must have consent to obtain information, and in order to have consent (whether express or implied) organizations must identify the purposes for which personal information is collected at or before the time of collection
 - Organizations shall not collect personal information indiscriminately; the amount and the type of information collected must be limited to that which is necessary to fulfil the identified purposes
 - Organizations using personal information for a new purpose shall document this purpose

Canada's Personal Information Protection and Electronic Documents Act


- The structure and foundational principles of the law is directed to business activities during which organizations must obtain a form of consent to obtain personal information and to use and disclose that information in order to provide products or services to consumers

Canada's Personal Information Protection and Electronic Documents Act

- PIPEDA does give consumers a right to control the use/disclosure of their personal information that is collected by businesses in the course of offering products and services. Fair information principles include:

- The ability to withdraw consent subject to legal and contractual restrictions
- The right to correct inaccurate information
- The obligation to retain data only so long as necessary for the purposes for which the information had originally be collected

Canada's Personal Information Protection and Electronic Documents Act

- Canada's Privacy Commissioner applies these concepts to content/service providers. In [PIPEDA Report of Findings #2015-002](#): the website [Globe24h.com](#) republished Canadian court and tribunal decisions and allowed the information to be indexed by search engines, and then charged a fee to have the personal information removed.
- The Commissioner held that this was not a reasonable use of personal information nor did [Globe24h](#) have appropriate consent to use the information in the court decisions in this way.
- The merits of the decision may be open to debate but the focus is on the content provider and its deliberate collection of personal information for commercial purposes 

- If PIPEDA and substantially similar laws *were* interpreted to apply to the generation of search results the laws would be subject to constitutional challenge
- In the case of PIPEDA, there is a constitutional division of powers limitation. The federal authority to enact PIPEDA is founded in the trade & commerce power and therefore the “commercial activities” limitation is constitutionally dictated
- This way raised in the *State Farm* case but not considered by the Court

Canada's Personal Information Protection and Electronic Documents Act

- The Canadian *Charter of Rights and Freedoms* also imposes limits on both federal and provincial law, most notably not to infringe the guaranteed right to freedom of expression and freedom of the press:
 - In *Alberta (Information and Privacy Commissioner) v. United Food and Commercial Workers, Local 401, 2013 SCC 62*, a union videotaped employees crossing a picket line. Individuals filed complaints under the Personal Information Protection Act.
 - The Court held that none of PIPA's exemptions allowed the Union to collect, use and disclose personal information for the purpose of advancing its interests in a labour dispute. However, the Court held that the restrictions on a union's ability to communicate and persuade the public of its cause imposed by PIPA violated the *Charter* right to freedom of expression

Canada's Personal Information Protection and Electronic Documents Act

- In [*Crookes v. Newton*, 2011 SCC 47](#), the Supreme Court did not address automatically generated search results but recognized the indispensability of hyperlinks:
 - “The Internet’s capacity to disseminate information has been described by this Court as “one of the great innovations of the information age” whose “use should be facilitated rather than discouraged” ...Hyperlinks, in particular, are an indispensable part of its operation. As Matthew Collins explains, at para. 5.42:
“Hyperlinks are the synapses connecting different parts of the world wide web. Without hyperlinks, the web would be like a library without a catalogue: full of information, but with no sure means of finding it.”
- Similar to Hyperlinks, search engine results obviously are indispensable to the ability of individuals to use the Internet in any meaningful way

Unlawful Use of Personal Information

- Canadian law provides several means to prevent unlawful uses of personal information such as:
 - Invasion of Privacy Torts: common law and statutory
 - Defamation
 - Criminal Law
- these causes of action are directed at intentional or unlawful misuse of information. They do not provide any basis for removal of information simply because it is inaccurate, irrelevant, or excessive
- these causes of action also have no direct application to search engines but rather are directed at the parties who have perpetrated the tortious or unlawful act

Common Law and Statutory Torts

- the common law and statutory torts give individuals a right of control over their personal information but require an intentional and offensive invasion of privacy
- Recognition of a common law tort relating to invasion of privacy is relatively new though related torts (eg appropriation of personality) have long existed
- In [*Jones v Tsige*, 2012 ONCA 32](#), the Court recognized a tort of “intrusion upon seclusion” that has the following elements:
 - The defendant’s conduct must be intentional
 - The defendant must have invaded the plaintiff’s private affairs or concerns without lawful justification
 - A reasonable person would regard the invasion as highly offensive

Common Law and Statutory Torts

- In *Jones*, the Court acknowledged that other categories of “invasion of privacy” torts may be recognized in future including public disclosure of embarrassing private facts about the plaintiff or publicity which places the plaintiff in a false light in the public eye.
- All of these categories of tort have their origin in the United States’ invasion of privacy tort categories which requires a high standard of “offensiveness”. It is notable that, in the US, the invasion of privacy tort does not apply to publication of truthful information that is obtained from public official court records (see *Gates v. Discovery Communications, Inc.*, 101 P. 3d 552 Cal: Supreme Court 2004))

Common Law and Statutory Torts

- The statutory torts are similarly limited to intentional invasions of privacy (intention is the hallmark of a tort). In [*Douez v. Facebook, Inc.*, 2014 BCSC 953](#) the BC Court explained that the Privacy Act categorizes two torts:
 - Invasion of privacy, which could include intrusion on seclusion, public disclosure of embarrassing private facts, or publicity which places the plaintiff in a false light in the public eye
 - misappropriation of the name or likeness of a person for commercial purposes

Common Law and Statutory Torts

- In *Douez*, the plaintiffs in a class action have raised the misappropriation tort, alleging that Facebook took the names and images of Facebook users in British Columbia and featured them in advertisements sent to the users' contacts, without the knowledge or consent of the person featured in the ad
- There is no Canadian jurisprudence that holds a search engine liable for committing the tort of invasion of privacy, nor is there any reported case where a plaintiff who has obtained an order for invasion of privacy has sought to have that order enforced against a search engine, as a non-party.

- Defamation is a common law tort the elements of which are publication to a third party of a false and defamatory statement that identifies the plaintiff
- There are several available defences including fair comment, qualified privilege, public interest responsible communication and absolute privilege
- In *Crookes v Newton* the Supreme Court of Canada held that a hyperlink, by itself, should never be seen as “publication” of the content to which it refers. The Court did not specifically consider the status of automatically generated search results

- In the recent decided case [Niemela v. Malamas, 2015 BCSC 1024](#), the plaintiff had obtained an order against the publisher of defamatory content. Google had voluntarily removed “.ca” search results that contained snippets of the information.
- The plaintiff sought an injunction requiring Google to block search results worldwide. The plaintiff also sued Google for defamation, injurious falsehood and breach of privacy.

- The Court in *Niemela* held:
 - The injunction was not warranted as:
 - There was no irreparable harm associated with the non “.ca” search results
 - Google would not be able to comply with an Order requiring it to block search results in the US due to laws that block enforcement orders that would infringe on the First Amendment right to free speech
 - The case was distinguishable from the “extraordinary” circumstances in *Equustek Solutions Inc. v. Jack* (leave to appeal currently before the Supreme Court of Canada) in which the BC court required a non-party search engine to delist search results worldwide to enforce a court order relating to illegal counterfeiting activities

- In *Niemela*, the defamation case against Google was dismissed on the basis that:
- following the precedent established by *Crookes v. Newton*, Google could not be considered the publisher of the defamatory content but rather was a passive instrument.

- The facts accepted by the Court included that:
 - (a) Search results and ‘snippets’ on Google’s websites are generated automatically through the operation of computer algorithms in response to search terms inputted by users.
 - (b) Google’s proprietary algorithm is programmed by Google to rank search results according to their probable perceived relevance to users.
 - (c) Google maintains different search platforms for different countries and search results may vary from platform to platform.
 - (d) The search results generated by the algorithm are generated from the automated review of more than 60 trillion websites. They are continuously updated and may vary from hour to hour or even from minute to minute.

- The facts accepted by the Court included that (con't):

(e) Google's search platforms provide a means for internet users to locate websites hosted by third parties that may be of interest to the user.

(f) Google does not promote or endorse particular search results. It neither warrants the reliability of websites generated in search results nor cautions the user that the authors of statements found on websites may not be trustworthy.

(g) Google does not amend search results for commercial gain.

(h) A single page of search results generally displays 10 results, with hyperlinks to third party websites accompanied by snippets of text from those sites. More results are displayed on further pages.

- The facts accepted by the Court included that (con't):
 - (i) Pages may include third party advertising which is identified as such.
 - (j) Search results reflect the content of third party websites at the time the sites were last crawled by the computers processing Google's search algorithm. Changes in the site by the third party host may not be reflected in search results until the page is crawled again by Google's computers processing the algorithm. Google does not control the content of third party websites, nor changes to those websites.

- The Plaintiff had no facts to rebut the passive instrument test, particularly since Google had voluntarily blocked the “.ca” search results when notified of the court order obtained by the Plaintiff
- The other tort based claims were also dismissed:
 - there could be no reasonable expectation of privacy of content relating to how the Plaintiff performed his professional work (it was in essence a “dressed up defamation” claim)

- While Canadian law does give individuals a right to control the use of personal information for commercial purposes and to protect against unlawful usages of their information, there is no basis in Canadian law for the concept of the “Right to Be Forgotten” adopted by Europe in the *Gonzalez* decision
- Any adoption of the European style “Right to Be Forgotten” would be subject to the Canadian Constitution and *Charter of Rights and Freedoms*, and most notably, the constitutionally guaranteed right to freedom of expression
- Of particular concern is the French privacy regulator’s extension of the European conception of the “Right to Be Forgotten” to all geographical extensions (i.e. domain names) worldwide: as countries such as Russia adopt “Right to Be Forgotten” laws, should they be entitled to dictate the information available to you?

Thank You

Wendy J. Wagner

613-786-0213

wendy.wagner@gowlings.com

gowlings

Lawyers • Patent and Trade-mark Agents

montréal • ottawa • toronto • hamilton • waterloo region • calgary • vancouver • beijing • moscow • london