



Volume 15

Spring

2019

djim.management.dal.ca |

The Right to be Forgotten: The Potential Effects on Canadian

Steven McDonald

School of Information Management, Dalhousie University

Abstract

Since the introduction of the right to be forgotten to European law in 2014, many Western countries have contemplated whether the right could be applied to their citizens. In October 2018, Canada's Privacy Commissioner asked the Federal Court of Canada to decide if the right is a Canadian fundamental right. However, the right to be forgotten has caused a lot of issues in Europe due to its vagueness and if Canada's Federal Court rules in favour of making the right a Canadian right, changes will need to be made to it to protect Canadian archives. This paper explores the right to be forgotten and discuss the potential effects the right may have on Canadian archives by exploring the origins of the right, how third-party search engines are currently handling the right, Canadian laws and policies surrounding privacy and the right to know and Canadian archival practices.

Introduction

What started as a small court case in Spain quickly spread across the world; the right to be forgotten – or sometimes referred to as the right to be erased – has generated a lot of conversations in many countries throughout the world. Currently, the right to be forgotten is only used within

European Union (EU) nations but many governments have started to debate whether the right can be applied within their countries. For example, in October 2018 the Canadian Privacy Commissioner – Daniel Therrien – asked the Federal Court of Canada to decide if the right to be forgotten should become a fundamental

right for Canadians (Thomson, 2018) and they are expected to decide in 2019. In 2014, the Australian Law Reform Commission ruled against the right but due to social pressures the Commission has reopened its investigation into the application of the right (Lavoipierre, & Smiley, 2018).

But what is the right to be forgotten? Currently, the right to be forgotten only affects third party search engines that operate within Europe such as Google, Yahoo, and Bing. According to the EU, these search engines are considered to be "data controllers" and have special obligations in the EU that include in the removal of out-of-date information (Arthur, 2014). In other words, EU residents can request third party search engines operating within Europe to remove out-of-date or irrelevant information about themselves from the search engine's indexes. In more simpler terms, John Smith could request Google to remove his name from a website link's index.

Although the right can only be applied to online search engines, many worry that it could lead to the removal of information outside of search engines and be applied to other websites such as Wikipedia or be transferred to paper documents within records management and archives. Many public figures in the United States of America (USA) have stated their opinions and worries about the right. In an interview with Bloomberg (2018), Rep. Ro Khanna – a California Democrat – stated that he

believed that the right to be forgotten is unconstitutional in relation to the United States' first amendment (the freedom of speech) and may be taken advantage of. Jimmy Wales – a co-founder of Wikipedia – tweeted his concerns about the EU decision affecting Wikipedia pages due to someone not liking the information on the page (2014); and Jeff Jarvis – a professor at City University of New York – also tweeted his opinion regarding his belief that the right goes against free speech (2014).

These opinions show that there is a cultural divide about the right, whereas many European residents believe the right is a good idea and does not violate any free speech rights while residents outside of Europe, mostly individuals from the USA, have stated their worries about the effects that the right to be forgotten will have on their rights. It also shows that there is a lot of confusion surrounding the right and what the right can affect. This paper will explore the right to be forgotten and discuss the potential effects the right may have on Canadian archives, if the right was ever to be applied to paper documents, by exploring Canadian laws and policies surrounding privacy and the right to know and Canadian archival practices. The paper is divided into three sections. The first section explores and discusses the right to be forgotten in Europe and in Canada and the second section explores Canada's privacy and information laws and determine whether the right to be forgotten can take effect in Canada. The

third section discusses whether the right to be forgotten can be applied to Canadian archives and what archivists can do to prevent information from being removed from their collections.

Section I: The Right to be Forgotten

The Story Behind the Right to be Forgotten

Discussions about individual information rights have been occurring in Europe since the dominance of the World Wide Web. Although at the time it was not called the right to be forgotten, the ideology was beginning to form within the EU with its Data Protection Directive (1995), often referred to as Directive 95/46. The directive's goal is to protect the privacy of residents of any EU nation and set regulations for the movement of said information between EU nations. Section two of the directive states that data processing systems must respect the fundamental rights and freedoms of an individual especially their right to privacy within reason.

Although the directive pre-dates the rise of the World Wide Web, it would become the standing argument for a 2012 Spanish court case. On March 5th, 2010, Mario Costeja Gonzalez of Spain lodged a complaint against La Vanguardia Ediciones – a daily newspaper with a large Spanish viewership – Google Spain, and Google Inc. The complaint was based on an individual Google searching Gonzalez's name, which linked to two La Vanguardia digitized

newspapers from January 19 and March 9, 1998 presenting advertising real-estate auctions with information that the buildings were taken away from Gonzalez and his family due to debt (Court of Justice of the European Union, 2014).

Gonzalez argued that the information within the advertisements should be considered out-of-date because he was no longer married and no longer in debt. But whenever someone searched his name in Google, links to these digitized ads would be the first to appear on Google which has been affecting his legal business (La Vanguardia, 2014). During the trial, Gonzales requested that La Vanguardia remove or alter the digital pages so that his personal information will no longer appear and requested that both Google either remove or conceal the links to those digitized news ads. The courts ruled against Gonzalez' request for La Vanguardia's removal or changing of the ads due to European copy right laws and archival processes but did rule in favour of Gonzalez' request for Google to remove or hid the links (Court of Justice of the European Union, 2014).

Google tried to appeal the court's decision, but the National High Court stood by the court decision referring to Article 12 (b) in the European Parliament's Directive 95/46 which states "erasure or blocking of data the processing of which does not comply the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" (para. 1) and article 12

(c) "third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b)" (para. 1). The National High Court also referred to Article 14 (a) of the Directive which states "object at any time on compelling legitimate grounds relation to his particular situation to the processing of data relating to him" (para. 1). The National High Court believed that the articles can and should be applied to search engines and other third parties web pages. It was during this National High Court's decision that the Right to be Forgotten was coined.

Another controversial ruling happened in 2016 when a Belgian court ruled in favour of the removal of a digital copy of a Belgian newspaper, *Le Soir*, article from 1994. In 2008 *Le Soir* made a large portion of its digital archive available online. One of the archived newspapers released had an article from 1994 about a car accident containing the full name of the individual accused of being responsible for the accident (Vavra, 2018). Sometime during May 2016, the named individual brought *Le Soir* to court requesting that their name be removed from the digital article and from the newspaper's index. The court ruled in favour of the individual stating that because there was no criminal offence charged to the individual, the name should have never been released and deemed that the information has become irrelevant (Van Eecke, 2016).

What did these rulings mean for the rest of the European Union? Because of rules

outlined in Article 13(5) paragraph 2 of the Treaty Establishing the European Community (1957) which states that EU nations must harmonize their laws and regulations to allow for a more open market and freedom of movement. Every nation within the EU must allow any EU resident to exercise their right to be forgotten and request third party search engines, like Google, to either remove or hide links related to information about them. Thus, shortly after the court ruling, EU residents started filing for search engines to remove or hide information about themselves.

The Processes of Removing Information from Google

Google's Transparency Report (2018) states that the search engine has received over 740,000 requests to delist comprising over 2.8 million URLs requests to be delisted. But what does Google do with all those requests? Before Google could do anything with the requests, it needed to create policies and guidelines that ensured that each request was processed equally and complied with Article 29 of the Working Party's guidelines which, in May 2018, was replaced by the European Data Protection Board (EDPB). To complete this task, Google created The Advisory Council to Google on the Right to be Forgotten shortly after the court case.

The Council's job was to seek advice from EU experts on privacy and information and have them meet up and discuss how Google should handle the right to be

forgotten. The Council held seven public meetings across the EU – Madrid, Rome, Paris, Warsaw, Berlin, London, and Brussels – in late 2014 with the goal to aid Google in determining how to approach the more “grey area” requests between the right to information and the right to privacy, such as requests asking for the removal of an individual’s name from a webpage link that states that individual’s past crime from 10 years ago and if the individual has not committed a crime since then. Experts outside the Council and the public could state their opinions and worries about the right at these meetings which would allow Google to create a fairer approach in assess requests (Google Advisory Council, 2015). The Council published its report on February 6, 2015.

The Council determined that the best course of action for Google is to assess each request on a case-by-case basis and determine if the webpage has information related to public interests. This method has allowed Google to delist 44.0% of the 2.8 million (about 1.2 million links) URLs requested to be removed from its search index (Google, 2018a). The benefit to this method is that it allows Google to determine the solution equally and provides the requestee a report that lists reasons for the removal, or for not removing, the link(s) from its index. The guideline provides a few examples of when Google will not delist links: the information is related to past crimes (depending on the severity of the crime), political office,

position in public life, self-authored content, consists of government records, and journalistic rights (Google Advisory Council, 2015).

Another benefit of assessing each request case-by-case is that it allows Google to consider the rights of the requestee and public interest of the individual. This allows Google to have a better control over the process and ensures that individuals are not taking advantage of having information about themselves removed from being seen by the public. Google received a request to delist 29 URLs from an individual who once held a position of power at a major company within the United Kingdom (UK) and went to prison due to attempted fraud; Google did not delist 21 of the URLs because the information was deemed to have enough substantial public interest to the individual’s personal life but it did delist three URLs because the requester’s name was not listed on the page. The final five pages could not be found through Google searches (Google, 2018a).

Even though Google has been following the EU court’s ruling, the National Commission for Informatics and Liberties (CNIL) is not satisfied with Google’s effort in the removal of links with personal information from all its search indexes. Currently, Google only removed requested links from either that nation’s version or EU’s version of Google and not from every version of Google operating in every nation (Meyer, 2018). This means that it is possible for someone in another country to access

the “removed linked” and view the personal information. The CNIL wants Google to apply the delisting to all versions of Google inside and outside of the EU; it believes that if someone has requested to be delisted from a link, nobody should have access to that link (Meyer, 2018). Google’s actions show that the company wants to adhere to the right and work with the EU to create a solution but the CNIL believes that Google is not acting fast enough and does not care about the right and thus should be punished by EU authorities (Lecher, 2019).

Section II: Canadian Privacy and Information Laws

Canadian Privacy Laws

There are several federal and provincial laws in Canada that oversees the use of personal information in business and online, but this paper will only focus on Canada’s two largest privacy policies – the Privacy Act and the Personal Information Protection and Electronic Documents Act (PIPEDA). The Privacy Act was created in 1983 to provide guidelines on how federal government institutions deal with the personal information of individuals. Some of the provisions of the legislation include how government institutions collect personal information, which institution can collect what type of information, disclosure of the collected information, informing an individual about the purpose of the information being collected, and individuals having the right to access their information (Parliament of Canada, 1983). The Act only applies to the 147 federal

government institutions listed in section 3 of the Privacy Act: Schedule of Institutions.

PIPEDA was introduced in 2000 as a federal privacy law that controls how businesses collect, use, or disclose personal data information for commercial activities except for journalistic, artistic, or literary purposes. The biggest difference between PIPEDA and the already in place Privacy Act is that PIPEDIA only controls private businesses within Manitoba, New Brunswick, Newfoundland and Labrador, The Northwest Territories, Nova Scotia, Nunavut, Ontario, PEI, Saskatchewan, and Yukon. PIPEDA does not cover not-for-profit and charity groups, political parties, municipalities, universities, schools, or hospitals unless the personal information crosses provincial borders (Parliament of Canada, 2000). Alberta, British Columbia, and Quebec have their own private-sector laws that the federal government has deemed to be similar enough to PIPEDA.

PIPEDA provides the individual with the right to know why an organization is collecting their information, how that organization will use their information, what the organization’s responsibilities are for the collected information, access to the collected information, and allows individuals to ask for corrections and complain about how an organization handles their personal information. The Act requires organizations to obtain consent before collecting an individual’s information, not disclose an individual’s information even if the said individual

refused consent, collect information within the realms of Canadian laws, and provide clear and understandable policies about how the organization uses and collects personal information (Parliament of Canada, 2000). On June 18, 2015, the Government of Canada introduced the Digital Privacy Act as an amendment to PIPEDA to include mandatory breach notification for businesses, increase fines of up to \$100,000 for businesses breaking privacy laws, enhance the authority of the Privacy Commissioner, and introduce a new exemption for business transactions (Parliament of Canada, 2015).

Both privacy acts recognize any factual or subjective information about a person is personal information; this includes age, name, income, ethnic origin, blood type, opinion, social status, employee files, credit records, and medical records. However, the acts do not recognize non-subjective information about an individual (for example, postal codes), information about an institution or business, anonymous information, certain information about public servants (names, position, and title), government information, and a person's business contact information (Office of the Privacy Commissioner of Canada, 2018).

None of the Canadian privacy laws currently recognize the right to be forgotten, but on October 10, 2018, Daniel Therrien – Canada's Privacy Commissioner – asked the Federal Court of Canada to decide if the right to be forgotten can be applied to Canadians (Thomson, 2019), the

Federal Court has yet to come to a decision. Therrien's biggest query was about whether the PIPEDA affects third party search engines as well as an individual's right to request the delisting of links from search engines and whether PIPEDA needs another amendment to include the right to be forgotten (Chhabra, 2018). This means that if the Federal Courts recognizes the right to be forgotten as a fundamental Canadian right, third party search engines will need to change their removal policies within Canada.

Access to Information Act

The federal government of Canada introduced the Access to Information Act (1985) to provide Canadian residents the right to access information in government records with the principle that information created by the government should be available to the public with some exceptions due to personal information and national security. This "freedom of information" law provides residents the chance to request information from government institutions and receive notice of the decision of the request within a reasonable time and cost. Most provinces and territories have introduced their own freedom of information laws affecting provincial jurisdictions.

In Canada, access to information laws and privacy laws are closely connected. Government institutions must consider what type of information is within the requested record. The record cannot have

any personal information of someone other than the individual requesting the record.

Can Canadians Remove Personal Information from Google?

Even though the right to be forgotten is not currently applied to Canadians, Google allows Canadians to request the removal of links revealing personal information such as bank account numbers, images of their handwritten signature, and explicit images or videos that have been released without their consent from Google search results. But if the individual wants personal information to be removed from the website itself, they must ask the website's owner to remove the information (Google, 2018b) or report the institution to the Office of the Privacy Commissioner of Canada.

Although Google Canada does not provide the same level of service in the removal of personal information from its index, by applying the guidelines currently used in the EU, Google could provide Canadians with the right to be forgotten. As mentioned earlier, the right to be forgotten only applies to personal information that is no longer necessary, correct, out-of-date, or excessive. Google already allows Canadians to request the delisting of links that reveal personal information such as a handwritten signature or explicit photographs and videos; thus, allowing Canadians to request to delist their name from links that disclose personal information would not be too much trouble for Google.

Section III: Archive and the Right to be Forgotten

The Right to be Forgotten in the Archival Setting

Since the introduction of the right to be forgotten in the EU in 2014, many experts have expressed their worries about the implication the right may have in other parts of the internet (Google Advisory Council, 2015). Although the right to be forgotten cannot be applied to paper records held within archival repositories, it has been applied to digital formats of paper records, such as the case of the Belgian court ruling mentioned earlier. The vagueness of the right and how every European nation has a different understanding of what the right to be forgotten is, has proven to be the biggest problem for digital archives.

Digitization is the process of scanning physical archival records into electronic formats to be accessed online or within the archival network. Any archival metadata about the physical record is transferred with the digital copy and inputted into the archival digital database. It is important that the metadata is transferred properly to ensure easy access for the public and archive employees, thus an index might be created to allow for easier searches (U.S. National Archives and Records Administration [NARA], 2004). Digitization is not used as a preservation method but as a way to promote the records within the archival institution. But the Belgian Supreme Court ruled that digital copies of historical records within a private

company's website also fall under the right to be forgotten which raises questions and concerns about where the right to be forgotten can be applied.

What can Canadian Archives do?

The right to be forgotten cannot be applied to paper records but as seen earlier it can be applied to digital archives and with digitization being major projects for archival institutions in Canada, many archivists are worried if their digital content will be affected by the right. Ashley Vavra (2018) suggests that there are three major concerns archivists have about the right to be forgotten. The first is the vagueness of the law which allows every EU nation to interpret the law differently as has been seen earlier with the Belgian case. The second concern is the laws surrounding the transparency third party search engines must follow. Google has tried to be as transparent about its decision-making process, but the EU has never been satisfied with Google's transparency. The third concern is about access to information and how the right to be forgotten restricts this access. Archivists often cite Article 19 of the Universal Declaration of Human Rights, which states that everyone has the right to seek and receive information and argue that the right to be forgotten goes against the Article.

If the right to be forgotten is accepted by the Canadian Federal Courts and becomes a Canadian right, the best way to protect archival records is by advocating for better

terminology and definitions. The International Federation of Library Associations and Institutions [IFLA] (2012) Code of Ethics, states that it is the responsibility of information managers to advocate to ensure that the right of accessing information is not denied and advocate and negotiate for better access to information without the fear of being hindered by governmental and institution laws and policies. Advocating for the Canadian government to clearly define what the right to be forgotten is and where it can be applied to would benefit everyone. By providing clear definitions to the right, the government can reduce possible abuse about the right by providing a list of where the right can be applied and where it cannot be applied.

If the Canadian Federal Courts recognize the right but do not provide clear terminology, archivists should be worried about the possible effects the right may have on archival collections. Archivists can ensure archival institutions are not affected by sticking to the archival fundamental principle of respect des fonds. Respect des fonds is the principle that the records of a person, family, or corporate body must be kept together in their original order and not be mixed or combined with the records of another fond. By continuing these practices, archivists can ensure that the right to be forgotten has as small affect as possible. Respect des fonds ensure that the records and information within a fond is kept in intellectual order and ensure

records and information is not removed and by continuing this practice, archivists can ensure that the information within a fond is not removed or lost due to the right.

Finally, archivists can respect requests from Canadian individuals to restrict information about themselves. Canadian archivists are familiar with the challenges with restricting material and records from being accessible to the public. Archives are repositories for government documents, business files, personal records, and other types of records all of which have the potential to contain information about individuals with or without their knowledge. This challenge has led archivists to create policies and guidelines for their repository focused on balancing access to the records and protecting individual privacy rights.

Restricting records is not a new concept for archivists and has been practiced since humanity started to write (Mount, & Newman, 1985) but determining which records get restricted and which ones do not has been a challenge for archivists. Many archivists agree that records should be restricted if they contain confidential information or sensitive personal information but argue often about what is considered confidential or sensitive information (McCarville, 2004). Sillitoe (1998) defined confidential information as information "obtained on an explicit or implied basis of confidentiality, from the individual to whom it pertains, or from a third party" (p. 9) and sensitive information as "[information] which would induce

substantial distress in a reasonable person if made publicly available" (p. 9).

Although Sillitoe provides definitions for confidential information and sensitive information, he does not provide examples. McCarville (2004) provides a large list of records that should be deemed to hold confidential information or sensitive information: Dominion census records after 1906, vital statistics, military personnel files, some government office records, record of post-secondary institutions, and hospitals are just some of the examples she lists. It is important to note that private donors can request restrictions be placed on the donated records. Most archivists advise the donor to request that certain records be restriction for a specific period of time or access be granted only with their permission instead of using the archive as a storage facility for their records and restricting access indefinitely. Archivists understand and respect privacy but placing an indefinite restriction on a fond does not benefit the public and takes up space within the archive.

A perfect example of an organization setting an indefinite restriction on it donated archive fonds is Statistics Canada. Statistics Canada argues that information collected in censuses is considered personal information and should never be released to the public. Statistics Canada often cites the Statistics Act which guarantees confidentiality of the information collected in census and expresses the fear that making census

information accessible will lower census return rates (Statistics Canada, 2000). Archivists believe that these records should be released to the public. They believe that the historical information stored on the records contain significant historical value and often cite census practices in the United States which release the collected data after 72 years and Britain which releases its collected data after 100 years (McCarville, 2004).

Conclusion

Although the right to be forgotten is useful in removing out-of-date, inaccurate, and personal information from third party search engines, there are many questions of what parts of the internet the right can be applied. In 2016, Belgium courts applied the right to a newspaper's digital articles thus allowing other EU courts to expand the usage of the right beyond Google.

Is the right to be forgotten a threat to Canadian archives? At this current moment, no, the right to be forgotten is not a threat to Canadian archives but if the Canadian Federal Court agrees with the EU decision and makes the right to be forgotten a Canadian right then it could become a problem, especially if the Canadian Government uses the same terminology and pretenses as the EU. The solution in preventing digital archives from being affected by the right to be forgotten is to advocate that the government clearly define what areas of the internet the right can affect. By advocating the government to remove the vagueness of the EU's

legislation, Canadian digital archives can feel a sense of safety knowing that their records will not be affected by the right and historical records will be accessible to everyone. Canadian archives already respect the privacy of individuals by restricting personal information about living or recently deceased individuals or following restriction requests from donors.

The right to be forgotten is a great idea and should be applied to Canadian third-party search engines. Allowing individuals to remove out-of-date, inaccurate, and personal information from Google search results allows individuals to feel a sense of ease knowing that none of their personal information will be presented within search results and not easily accessible. However, the right to be forgotten needs to be more clearly defined about where in the internet it can be applied and what information can be removed from search engines indexes.

References

- Arthur, C. (2014, May 14). Explaining the "right to be forgotten" – The newest cultural shibboleth. *The Guardian*. Retrieved from www.theguardian.com.
- Bloomberg. (2018, October 19). Rep. Khanna says EU "right to be forgotten" unconstitutional. *Bloomberg Technology*. Retrieved from www.bloomberg.com.
- Chhabra, S. (2018, October 10). Privacy watchdog asks federal court rule on Google de-indexing question.

- Mobliesyrup. Retrieved from www.mybilesyrup.com.
- Court of Justice of the European Union. (2014, May 13). Judgement in case C-131/12 Google Spain SL, Google Inc. v Agencia Espanola de Proteccion de Datos, Mario Costeja Gonazalez. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131>.
- European Parliament. (1995, November 23). Directive 95/46/EC of the European Parliament and 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. Official Journal 281, 0031-0050. Retrieved from <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX%3A31995L0046%3AEN%3AHTML>.
- European Union. (1957, March 25). Treaty establishing the European community (Consolidated version). Official Journal C 325, 0033-0184. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A12002E%2FTXT>.
- Google. (2018a, November 8). Transparency report: Search removals under European privacy law. Retrieved from <https://transparencyreport.google.com/eu-privacy/overview?hl=en>.
- Google. (2018b). Removing information from Google. Retrieved from <https://support.google.com/websearch/troubleshooter/3111061?hl=en>.
- Google Advisory Council. (2015). Read the Advisory Council's final report: How should one person's right to be forgotten be balanced with the public's right to information? Retrieved from <https://archive.google.com/advisorycouncil/>.
- International Federation of Library Associations and Institutions [IFLA]. (2012, August). IFLA code of ethics for librarians and other information workers (full version). International Federations of Library Associations and Institutions. Retrieved from <https://www.ifla.org/publications/node/11092>.
- Jarvis, J. (2014, May 13). EU's "right to be forgotten" is a blow against free speech. Gu.com/p/3p75b. [Twitter post]. Retrieved from www.twitter.com.
- La Vanguardia. (2014, May 14). Mario Costeja, the Spaniard who defeated the almighty Google. La Vanguardia. Retrieved from <https://www.lavanguardia.com/tecnologia/internet/20140514/54407>

- 896513/mario-costeja-google.html.
- Lavoipierre, A., & Smiley, S. (2018, July 23). The nightmare of mopping up your online reputation and the "right to be forgotten." ABC News. Retrieved from www.abc.net.au.
- Lecher, C. (March 1, 2019). Facebook, Twitter, and Google still aren't doing enough about disinformation, EU says. The Verge. Retrieved from <https://www.theverge.com/2019/3/1/18246526/facebook-twitter-google-social-media-disinformation-europe>.
- McCarville, J. (2004). Balancing access and privacy in archives: New challenges in the face of Canadian privacy legislation. *Feliciter*, 50(4), 149-153.
- Meyer, D. (2018, September 10). The "right to be forgotten," globally? How Google is fighting to limit the scope of Europe's privacy law. *Fortune*. Retrieved from www.fortune.com.
- Mount, E., & Newman, W. (1985). Top secret/Trade secret: Restricting and accessing information. *Collection Building* 7(2), 3-7.
- Office of the Privacy Commissioner of Canada. (2018, January 31). Summary of privacy laws in Canada. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/.
- Parliament of Canada. (1983, July 1). Privacy act (R.S.C., 1985, c. P-21). Retrieved from <https://laws-lois.justice.gc.ca/eng/acts/P-21/index.html>.
- Parliament of Canada. (1985, July). Access to information act (R.S.C., 1985, c. A-1). Retrieved from <https://laws-lois.justice.gc.ca/eng/acts/A-1/>.
- Parliament of Canada. (2000, April 13). Personal information protection and electronic documents act. Retrieved from https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/.
- Parliament of Canada. (2015, June 18). Digital privacy act (S.C. 2015, C. 32). Retrieved from https://laws-lois.justice.gc.ca/eng/annualstatutes/2015_32/page-1.html.
- Sillitoe, P. (1998). Privacy in a public place: Managing public access to personal information controlled by archives services. *Journal of the society of archivists*, 19(1): 5-15. DOI: 10.1080/00379819809514418
- Statistics Canada. (2000, January 6). Final report of the expert panel on

access to historical census records. Retrieved from <http://www12.statcan.ca/English/census01/Info/chief.cfm>.

Thomson, S. (2018, October 10). Will Canadians soon have the “right to be forgotten” online? Here’s what you need to know. Ottawa Citizen. Retrieved from www.ottawacitizen.com.

U.S. National Archives and Records Administration [NARA]. (2004, June). Technical guidelines for digitizing archival materials for electronic access: Creation of production master files – Raster images. Retrieved from <https://www.archives.gov/files/preservation/technical/guidelines.pdf>.

Van Eecke, P. (2016, June 3). Belgium: High court decision on the right to be forgotten. Technology’s Legal Edge. Retrieved from <https://www.technologysleageledge.com/2016/06/belgium-high-court-decision-on-right-to-be-forgotten/>.

Vavra, A.N. (2018). The right to be forgotten: An archival perspective. *American Archivist*, 81(1). 100-111. DOI: 10.17723/0360-9081-81.1.100

Wales, J. (2014, May 13). When will a European court demand that Wikipedia censor an article with truthful information because an individual doesn’t like it? [Twitter Post]. Retrieved from www.twitter.com.