

Memory Hole or Right to Delist?

Implications of the Right to be Forgotten for Web Archiving

Trou mémoriel ou droit au déréférencement ? Les implications du droit à l'oubli pour l'archivage du Web

Melanie Dulong de Rosnay and Andres Guadamuz

**Publisher**

Association Recherches en sciences sociales sur Internet

Electronic version

URL: <http://reset.revues.org/807>

ISSN: 2264-6221

Electronic reference

Melanie Dulong de Rosnay and Andres Guadamuz, « Memory Hole or Right to Delist? », *RESET* [Online], 6 | 2017, Online since 30 October 2016, connection on 19 November 2016. URL : <http://reset.revues.org/807> ; DOI : 10.4000/reset.807

This text was automatically generated on 19 novembre 2016.

© Association Recherches en sciences sociales sur Internet

Memory Hole or Right to Delist?

Implications of the Right to be Forgotten for Web Archiving

Trou mémoriel ou droit au déréférencement ? Les implications du droit à l'oubli pour l'archivage du Web

Melanie Dulong de Rosnay and Andres Guadamuz

Introduction

- 1 The theoretical conflict between the continental European conception of privacy, more protective of the individual, and the Anglo-Saxon point of view, in favour of public knowledge, was revived by the *Google Spain* “Right to be forgotten” (RTBF) case of 2014, which keeps attracting a sizable amount of academic commentary (Powles and Larsen, 2014). The leading search engine now has an obligation “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”, even if the information was lawful.
- 2 The legal obligation arising from this case may conflict with preservation and may prevent archiving. Wikipedia, that can be considered as a memory institution preserving knowledge and heritage, has vocally opposed the ruling through the voice of Wikipedia founder Jimmy Wales, Lila Tretikov, then Wikimedia Foundation Executive Director (2014), General Counsel Geoff Brigham and Legal Counsel Michelle Paulson. They fear that the removal of links will create censorship, “memory holes” (Wales, in Curtis & Philipson, 2014), and that the decision would be “undermining the world’s ability to freely access accurate and verifiable records about individuals and events” (Tretikov, 2014). Other, mostly US legal scholars with a libertarian vision of freedom of expression, more extensive than the European conception mindful of privacy, also strongly opposed the ruling, fearing that the right could “destroy the Internet archive and become a way to bury evidence” (Levine, 2014) or permit “Orwellian airbrushing of history” (Lyons, 2014). In October 2016, the Wikimedia Foundation filed a petition¹ with the French Conseil d’Etat

(higher Supreme Court) against a decision of the French data protection authority (CNIL²) “that Google must remove information globally from its search results when requested appropriately by French citizens”, on the ground that delisting would indirectly impact Wikipedia through Google search results.

- 3 Collective rights to remember and to memory, free access to information and freedom of expression seem to clash with private individual rights to privacy. The present article studies, with a socio-legal and techno-legal perspective, the possible impact of the “right to be forgotten” (RTBF) on the preservation of native digital heritage. It analyses the extent to which the ruling may affect archival practices, and whether resources may become impossible to preserve for future generations, risking disappearance from memories and history as no version would be available in public or private archives. We demonstrate that the RTBF, even if it can be criticized on many other aspects (such as the privatisation of quasi-judicial decision, the lack of process transparency, and the reinforcement of a quasi-monopolistic hegemony of the search engine on freedom of information), the ruling as such is not likely to prevent preservation. The recent legal provision of the right to erase should not conflict with archiving, statistical, scientific, and historical research purposes in order to balance privacy with the public interest. We contend that the RTBF name is misleading, as the content is not removed from the online space, but merely delisted from search results. Thus, the digital resource does not disappear, it remains available on the web and can be further analysed and disseminated.
- 4 In a first socio-legal part (part 2), after a presentation of core legal concepts of privacy, data protection and freedom of expression, we analyse the case and the right to be forgotten, and look deeper into the controversies that have been generated by the decision.
- 5 Then, in a second techno-legal part (part 3), we explore the concrete implications of the decision on web archiving. The RTBF is not the only problem facing web archiving, other challenges and regulations exist to remove content. After a presentation of the existing techno-legal arsenal to delete, we will explain that web crawlers do not archive everything and point to the more pressing issues facing web archiving.
- 6 Finally, we explore the impact of the newest version of the RTBF, which will be implemented during 2016 in the European General Data Protection Regulation and actually mentions web archiving. We look at the detail of the new ‘right to erase’ contained in the Regulation, and we comment on a proposed exception for archiving in the public interest. We conclude with the broader challenges raised by privacy-by-design and the technical enforcement of ‘digital forgetting’.

The socio-legal context

Privacy, Data Protection and Freedom of Expression: legal concepts as cultural constructs

- 7 In a video about surveillance and privacy, French activists La Parisienne Libérée and Jérémie Zimmermann remark that “everyone has something to hide” (Zimmermann & la Parisienne Libérée, 2014). It can be something innocuous, like a mild Farmville addiction, a guilty musical pleasure, or an embarrassing viral video. Some things can be more serious, such as a sexting session that has been made public, an incriminating picture that

may seriously hinder future employment efforts, information about one's sexual orientation while living or working in a community that has low thresholds of tolerance; affiliation to a political entity or union. What if a link to that sensible personal information was made available online for the world to see? Could you have a legal recourse to remove it?

- 8 As a response, Europe has a robust system to ensure the protection of personal data. Article 8 of the European Convention of Human Rights (ECHR) clearly specifies that “everyone has the right to respect for his private and family life, his home and his correspondence.” The main embodiment of this principle can be found in the application of the 1995 European Data Protection Directive (DPD), which enables the information self-determination³ of European citizens (Bygrave, 2002). The Data Protection Directive has the main objective of safeguarding the rights of an identified or identifiable natural person (known as a data subject), by setting a number principles and situations in which any information relating to the data subject (known as personal data) can be processed lawfully. Any legal entity that can determine the purpose and means of controlling a subject's personal data is known as a data controller.
- 9 The existing Data Protection Directive regime received in 2016 an update in the shape of the General Data Protection Regulation (GDPR). This text updates most of the existing provisions contained in the Data Protection Directive in order to better accommodate data protection to the digital era. Specifically, the GDPR contains specific provisions regarding the right to be forgotten, which we will be covered in more detail in the next section.
- 10 The right to privacy and the data protection regime do not exist in a vacuum: a person's right to enjoy a private life can often clash with other rights, particularly the right to freedom of expression present in Article 10 of the European Convention on Human Rights. Over the years, this conflict between privacy and freedom of expression has been the source of countless legal battles in the courts (Bignami, 2008). There is a long list of cases that pit those two rights against one another, including the cases of *Douglas v Hello*⁴, and *Campbell v MGN*⁵, just to name a few.⁶ In these decisions, courts have tried to reach a balance between competing rights, which tends to be largely dependent on the facts of the case. As a general rule, courts have favoured an approach that places individual privacy above freedom of expression when the subjects are ordinary citizens, as in *Wainright v Home Office*⁷ and *Google v Vidal-Hall*.⁸ On the contrary, courts are generally more likely to side with the public interest to know and with freedom of expression in cases involving public figures, such as the aforementioned *Douglas* and *Campbell* decisions.
- 11 While European courts have tended to provide a careful balance of these two rights, this is not the case in the United States, where the traditionally strong protection of freedom of speech has its counterpart in a considerably weaker level of privacy safeguard (Charlesworth, 2000). Indeed, the U.S. has been following an almost opposed view of privacy to that present in Europe, what Werro calls the ‘right to inform’ (Werro, 2009), and others have gone as far as labeling the ‘right to remember’ (Balkam, 2014). This right does not exist in any legal sense, but the name neatly encapsulates the different approaches to privacy. While Europe has protected privacy to the point of creating a new right to be forgotten, the U.S. protects freedom of expression to the extent that it almost constitutes a right to remember.

- 12 This trans-Atlantic privacy conflict came to its climax in October 2015 when the Court of Justice of the European Union (CJEU) produced a landmark decision in the case *Maximilian Schrems v Data Protection Commissioner*. While the *Schrems* case does not pit freedom of expression and privacy directly, it does illustrate the divergence between the European Union and the United States' treatment of privacy, a conflict that may end up having important financial implications. It also serves to explain the very different reactions to the creation of the right to be forgotten.
- 13 The case involves Austrian law student and privacy advocate Maximilian Schrems, who initiated legal proceedings against the Irish Data Protection Commissioner because, as a European Facebook user, he signed up to the terms of use set by Facebook Ireland, the European subsidiary of the US company. Because he lives in Europe, he was concerned that his personal data would be sent to the United States, and he wanted European regulators to stop such a transfer.
- 14 The European Data Protection Directive includes a principle stating that personal data from European citizens can only be transferred to a third country if the recipient territory provides an adequate level of protection for that data. The level of adequateness is assessed according to several circumstances, including “the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.” It soon became clear that the United States could not comply with this principle, and as a lot of data was sent across the Atlantic, a solution had to be found. European institutions came up with a so-called “Safe Harbor” allowing the transfer of personal data to the United States without having to declare that US law complied with data protection requirements. The agreement, reached in 2000, allowed the transfer to companies in the US that signed up to the “Safe Harbor Privacy Principles”, a condensed version of the provisions contained in the Data Protection Directive. The companies also agreed that the US Federal Trade Commission (FTC) or other oversight schemes would hold them responsible for abiding by those principles.
- 15 The system had been working for 15 years without incident, but after Edward Snowden provided evidence of complicit actions by US technology companies on the mass-surveillance apparatus, Schrems alleged that this was evidence of a violation of the data protection principles. Therefore, Schrems wanted the courts to declare the Safe Harbor agreements invalid. The case made it all the way to the CJEU, which carefully considered the different rights involved, decided to agree with Schrems, and declared the existing Safe Harbor invalid because it clearly did not protect European citizens adequately. The Court considered that the Data Protection Directive had given Member States the power to create national authorities tasked with the obligation to determine how personal data is used. By relying on the Safe Harbor decision, the data protection authorities would not have the power to examine claims lodged by data subjects, which would erode the very core principles behind the data protection regime.

The right to be forgotten

- 16 The so called “right to be forgotten” (RTBF) relies on the idea that one has the legal right to remove information about oneself that is accessible online and that is potentially damaging to one’s enjoyment of a private life, or more accurately, to have it de-listed

from search engine results. Various authors have pledged for such a right in the last decade. In particular, Viktor Mayer-Schönberger has been a vocal advocate for a right that allows Internet users to remove undesired information from the network (Mayer-Schönberger, 2009). The argument is that the Internet serves as a perfect storage place for memories of all sorts, and some of these memories serve no purpose, and may even prove to be extremely damaging. While society could simply change to give lower credit to these memories, his argument is that there should be a right to delete unwanted information from public online spaces.

Context and ruling⁹

- 17 Since the early 1995, European law started to move towards this line of argument, and by 2014 the building blocks were already there. The Data Protection Directive gives data subjects a variety of rights that, in combination, can eventually give rise to the so-called right to be forgotten. Article 6 of the Directive imposes an obligation for data controllers to keep personal data “accurate and, where necessary, kept up to date”, and Article 12 permits data subjects to request for rectification, erasure or blocking of data that is incomplete or inaccurate, or where one of the following conditions has been met: a) the processing is unlawful; b) the data is no longer necessary in relation to the purpose for which it was collected; c) the data subject withdraws consent; d) the data subject objects to the processing (Szekely, 2012). All of these are important for the courts to create a right to be forgotten on the Internet.
- 18 A limited version of this right has now been enacted by the CJEU in the landmark ruling of *Google Spain v Costeja González* (C 131/12). This is the first case that directly applies existing data protection principles to the Internet. The case involves Mario Costeja González, a Spanish national, whose name was mentioned in a webpage from the Spanish newspaper *La Vanguardia* detailing a real-estate auction connected with proceedings for the recovery of social security debts. Whenever someone searched for his name, these pages came up near the top. Mr Costeja González filed a complaint with the Spanish Data Protection Agency (*Agencia Española de Protección de Datos*, AEPD) using his prerogatives under the Spanish transposition of the Data Protection Directive. Based on the aforementioned Articles 6 and 12 of the Data Protection Directive, Mr Costeja González requested the removal or alteration of the pages from *La Vanguardia*, and he also requested *Google Spain* to remove or conceal the personal data relating to him, so that they ceased to be included in the search results and no longer appeared in the links to *La Vanguardia*.
- 19 The AEPD denied the request regarding the newspaper *La Vanguardia*, alleging that the publication of such data was legally justified, and it is a common procedure to make such information public in the national press. However, the AEPD granted the order concerning Google, and required that search engine results involving Mr Costeja González should not include a link to the offending pages. In a 2010 decision, the AEPD considered that “operators of search engines are subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society.” Unsurprisingly, Google appealed the ruling to the national high court (*Audiencia Nacional*), which referred several questions to the CJEU asking for clarification as to the application of the Data Protection Directive.

- 20 The questions involved in this case are complex, but they can be summarized as follows. Is the operation of indexing and crawling the web¹⁰ an act of personal data processing? If the answer is yes, are search engines (and potentially web crawlers) data controllers, in the sense that they are under an obligation to protect personal data? If the answer is again yes, then can data protection authorities order a search engine (and potentially a web archive) to remove from their results links to websites where personal data has been published, without having to address those websites directly?
- 21 In other words, the question is whether search engines (and potentially web archives, also using a search interface and providing results) should be considered data controllers, and therefore whether they should provide users with tools to amend or remove listing to inaccurate personal data. The CJEU decided that:
- 22 Search engines are to be classified as processing personal data, and therefore are to be considered data controllers.
- 23 As such, search engines will be deemed to operate in the country by having an office, branch or subsidiary “for the purpose of promoting and selling advertising”.
- 24 As a data controller, the search engine will have an obligation “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”, even if the information displayed in that page is lawful.
- 25 When analysing a data subject’s request to remove links to a search result, authorities should balance the interest of the subject in accordance to her rights under the European Convention on Human Rights, the economic interest of the service provider, the role played by the data subject in public life, and the public’s interest to have access to the information.
- 26 The decision has universally become known as the “right to be forgotten”, which is technically incorrect. The ruling has not created a new right as such, it has simply applied to search engines the existing rights to rectification, erasure, blocking and objection which are present in the Data Protection Directive and were already applied to personal data gathered by public authorities or processed by private entities. The Advocate General stated as much when he commented in his opinion that “the Directive does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests.”¹¹ However, the Advocate General was of the opinion that the court should not extend these rights to search engines, which the CJEU eventually did.
- 27 This case seems to pit privacy against freedom of speech. Indeed, if a result cannot be found – even if it can technically be accessed to when performing another search query, based on other words than the name of the person (e.g. the facts or the date) – the practical effect will be obscurity. While the court does mention freedom of speech, and makes a few considerations about the ongoing balancing act between both, the main thrust of the legal opinion seems directed at the privacy issue. The Court comments:
- Indeed, since the inclusion in the list of results, displayed following a search made on the basis of a person’s name, of a web page and of the information contained on it relating to that person makes access to that information appreciably easier for any internet user making a search in respect of the person concerned and may play a decisive role in the dissemination of that information, it is liable to constitute a more significant interference with the data subject’s fundamental right to privacy than the publication on the web page.

- 28 In other words, there may be a privacy violation in a web page that shows up when the data subject's name is queried, but this is less important than the page actually showing up in search engine results when the name is queried. However, the court has left open the possibility of a case-by case appraisal by data protection authorities when asked to grant an order to remove search results:

[I]nasmuch as the removal of links from the list of results could, depending on the information at issue, have effects upon the legitimate interest of internet users potentially interested in having access to that information, in situations such as that at issue in the main proceedings a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter. Whilst it is true that the data subject's rights protected by those articles also override, as a general rule, that interest of internet users, that balance may however depend, in specific cases, on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life.

- 29 Notably, there have been a few decisions that support the interpretation that the right to be forgotten will be applied on a strict case-by-case basis. The most noteworthy case happened in the Netherlands, where a court used *Google Spain* to answer a request to remove links to potentially damaging information. A court in Amsterdam denied a request by the owner of an escort agency who was convicted for attempted incitement of arranging a contract killing, a matter currently under appeal (Spauwen & van den Brink, 2014). The subject wanted links to the reports of the crime removed from search results, but the Dutch court refused the request with an interesting application of the interaction between privacy and freedom of expression. The court commented:

The [Google Spain] judgment does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions (Spauwen & van den Brink, 2014).

- 30 This seems a rational interpretation of *Google Spain*, as its rationale was always to remove links that may cause an excessive invasion of privacy. The Dutch court concluded:

The claimant now has to bear the consequences of his own actions. One of the consequences of committing a crime is that a person can be in the news in a very negative way and this will also leave its tracks on the Internet, maybe even for a very long time. (Spauwen & van den Brink, 2014).

- 31 This type of approach will probably be followed by national courts in future cases, and the fear expressed time and time again by many commentators that *Google Spain* will be misused by criminals and other undeserving recipients may very well be unfounded.

Application of the ruling

- 32 The right to be forgotten mostly covers the type of information that is liable to affect significantly "the fundamental rights to privacy and to the protection of personal data" (Google Spain, 2014), and it specifically mentions that the court seeks to have a fair balance between those rights and the public's right to access information. In other words, the decision does not give an unlimited right to remove anything that we do not like from the Web, it simply gives users the right to request the removal of links to search results which may seriously infringe a person's privacy. In order to do so, Google has made available a search removal request form in which a subject may apply to exercise their

rights within the European Union. This means that currently, it is entirely up to Google to decide whether such a request will be met or not.

- 33 How is Google applying the RTBF? In 2015, the company released a transparency report for European privacy requests for search removals (Google, 2015). By this year, Google had received 249,915 requests, and had evaluated 907,057 URLs for removal, 58% of which were not removed. The requests came from all over Europe, but perhaps unsurprisingly, the company received more requests from the largest countries in the EU (France, Germany, UK and Spain), with the UK accounting for 18,597 alone. In the report, Google cites examples of requests received and how they were evaluated:

A victim of rape asked us to remove a link to a newspaper article about the crime. The page has been removed from search results for the individual's name. We received multiple requests from a single individual who asked us to remove 20 links to recent articles about his arrest for financial crimes committed in a professional capacity. We did not remove the pages from search results. "We received a request from a crime victim to remove 3 links that discuss the crime, which occurred decades ago. The pages have been removed from search results for her name. "An individual asked us to remove links to articles on the internet that reference his dismissal for sexual crimes committed on the job. We did not remove the pages from search results." (Google, 2015)

- 34 Assuming that this quick snapshot gives a representative picture of the request received by Google, there seem to be two main categories of complaints. Firstly, there are people who either have been convicted or are suspected of having committed a crime, and these requests seem to be usually denied. Secondly, there are requests addressing more serious privacy threats, such as the aforementioned rape victim; those requests are usually granted, and we could argue that in this regard the right to be forgotten is working as intended. However, this is a limited take on the actual application, as we do not have access to the entire number of requests.
- 35 It is important to point out that if the above is an accurate representation of the actual RTBF application, then it would at least operate in a similar manner to limited witness and victim protection legislation in many countries. For example, in the UK, some vulnerable victims of crimes are protected by the law, a protection that can be extended to censoring the press (Temkin, 2003). In the past, injunctions and gag orders attempting to keep information from the public eye have easily been circumvented with Internet searches, making it impossible to enforce them online (Mathiesson, 2010).
- 36 Google has also released a list of most links removed by the website that receives the requests. Most of the application of the RTBF is centered towards removal of social media posts, with the top recipient of removal requests being Facebook. The second top recipient of removal requests is a website called Profile Engine, which gathers information held about individuals online. However, let us emphasize again that this analysis rests entirely on the little information available from the Google transparency report. More data is needed for a better analysis of the true impact of RTBF on freedom of expression and the public interest.
- 37 Interestingly, another source of information for analysis of removal requests is to be found when third parties, which have had links to them delisted by Google, tell the public of such removals. The best source of information outside of Google at the moment is Wikipedia, as they have a reader-friendly transparency report that now includes RTBF request removals (see Wikipedia, Notices received from search engines). While these reports are an important source of information, they are limited as they only provide

detail of the pages that have been delisted, without indication of who actually made the request, or for what reason. At the time of writing, there have been 282 Wikipedia articles removed from search results by Google as a result of an RTBF request, with the Dutch and English version of Wikipedia having received the majority of delistings. No pattern can be identified by looking at the removed pages, as these include reality TV shows (see Wikipedia, *Temptation Island*), a porn actress (see Wikipedia, *Helen Duval*), a former criminal (see Wikipedia, *Gerry Hutch*), and a trans-gender winner of a reality show (see Wikipedia, *Nadia Almada*). In short, there may well be legitimate reasons to delist in these circumstances, but it is impossible to make a full assessment.

The legal controversy: RTBF vs. Freedom of Expression

- 38 Commentators around the world have both hailed and criticised the RTBF decision. On the one hand, opponents worry that the decision may interfere with free access to information, and that it will herald an era of abuse of these amendment orders, even if the court has specified that authorities should take into consideration the public interest aspect of the linked data (Zittrain, 2014). Supporters point out that there are valid reasons why a person would like some personal data not to show up when her name is searched, and that there should be a legal recourse to those whose privacy is being severely affected (Guadamuz, 2014).
- 39 Overall, the coverage of the RTBF has been surprisingly negative. Particularly, commentary in the press and US academia has heavily criticised the decision. This is a topic that once more unearths the growing chasm between the US and Europe when it comes to the interaction between privacy and free speech, with many US commentators seeing the RTBF as an infringement on free speech. A common denominator in the criticisms is that the RTBF is going to be used to bury information that should be remembered. For example, commentators accused the RTBF of favouring censorship and preventing freedom of information: “one person's right to be forgotten may be another person's right to remember” (Solon, 2014). Because Google does not host the data, it should not be responsible for it (Rosen, 2012). Indeed, Internet Service Providers managed to get safe harbour legislations limiting their responsibility. Concerns for culture and memory if archiving is hampered have also been raised: “The need to remember” also happens in “online spaces of remembrance” (Parmar, 2014).
- 40 Other authors have highlighted the vagueness of the right, stressing, for example, that “since the right to be forgotten is such an amorphous concept, when employed in the service of guarding one's reputation, it makes the task of balancing rights even more complicated” (Fazlioglu, 2013).
- 41 Finally, some commentators (Tréguer, 2015) have criticized the ruling as being a good example of the so-called “privatization of censorship” (Tambini, Leonardi & Marsden, 2008); this is because Google is given the power to determine which results should be removed, instead of this important function going to a court of law. However, if a user is denied the application, this could be litigated in court. While it is true that Google retains considerable control over the RTBF enforcement, users can indeed still appeal decisions to data protection authorities and/or the courts. The power of the national Data Protection authorities tends to be forgotten in the debate, and it has been boosted by the *Schrems* case.

42 This being said, the question of Google’s applications is perhaps the most important point of debate and an aspect of the ruling that has been lost in the privacy *versus* freedom of expression discourse. The current implementation of the RTBF rests considerably on a firm, who has the power to review the decision and deny the application, and who is directly responsible for existing unsuitable examples. This kind of power has led several academics to issue a request (Open Letter) to Google for more transparency about the way in which it applies the right. As Google has become such an important broker in this area, there is a growing need to understand the type of requests that are handled, and what parameters are being used to make decisions. This open letter says:

We all believe that implementation of the ruling should be much more transparent for at least two reasons: (1) the public should be able to find out how digital platforms exercise their tremendous power over readily accessible information; and (2) implementation of the ruling will affect the future of the RTBF in Europe and elsewhere, and will more generally inform global efforts to accommodate privacy rights with other interests in data flows. (Open Letter)

43 The RTBF could work mirroring an existing mechanism that helps to remove false positives, this is the notice and take down procedures for copyright infringing materials (Urban & Quilter, 2006). Over the years, content has been removed in Google services such as YouTube due to mistaken or malicious removal requests, only to be restored once the affected party has complained. It would be possible to deploy a similar regime for RTBF requests, both with more transparency and with a stronger system of protection for freedom of expression.

44 While some of these concerns are legitimate, some critics apparently fail to understand how limited the new right is in practice. As stated before, the CJEU tried to base their decision on privacy, leaving out most of the balancing act between privacy and data protection. There is something to be said about the political power of remembrance, particularly in countries that housed secretive and repressive regimes where people were “erased” from history; but we must understand the *Google Spain* decision as a much more nuanced allowance to delist information to protect privacy.

45 There has been a rush to assume that the right will affect data integrity and online archiving as mentioned in the introduction by Wikipedia founder and executives, or in a widely read blog (Hole, 2014); however, we argue that this is not what the ruling implies. The right mostly covers the type of information that is liable to affect significantly “the fundamental rights to privacy and to the protection of personal data”, and it specifically mentions that the court seeks to have a fair balance between those rights and the public’s right to access information. In fact, a large part of the debate so far was tainted by overlooking the precise wording of the ruling.

Implications of the RTBF ruling for web archiving

46 Web archival is faced with personal data in everyday practice, as soon as a document mentions the name of a person, but even when the person is not named but identified by characteristics that allow to deduce her name by association (Szekely, 2014).

Web archiving crawlers don't archive the entire web

47 Web archiving is facing other hurdles than the right to erasure. Web archiving started as early as 1996 with efforts to develop better crawlers and alternate between blind and selected crawling (Masanes, 2002; Brügger, 2011). Preservation is operated by private search engines and foundations (such as Internet Archive), public heritage institutions (national libraries) and also academics archaeologists and web historians in unstructured (Jeffrey, 2012) and structured manners:

Since the mid-1990s a number of international and national web archives have been founded, and easy-to-use web archiving software has been developed, thus enabling scholars to do their own web archiving(...) the most widespread is web harvesting, i.e. the retrieving of web material from web servers by the use of crawler software that 'crawls' the web based on a list of web addresses (URLs) to archive. (Brügger, 2012).

48 Commons-based solutions of peer archiving, such as the Day of Archaeology (Day of Archeology) initiative, are also developed to avoid the "digital dark age" of user-generated content (Jeffrey, 2012).

49 Because of the *Google Spain* ruling, the RTBF and the right to erasure, and the general practices and notice and takedown, web archiving will not preserve the entire web. Does that really matter beyond open data extremists, and "memory-maniacs"? (Parmar, 2014).

50 In reality, most of the content is not permanent. It disappears, sometimes even before it gets a chance to be archived: according to various studies, 85% within a year and 59% within a week (Ambrose, 2012), links get broken, hosting stops or dies, content gets overwritten. There is a "missing web" and web archiving is "almost always deficient" (Brügger, 2012). It has always been up to librarians, historians and archivers to choose what content, today on blogs and websites, is to be preserved in Internet Archives and National Libraries collections.

51 National libraries do not collect the entire web and do not rely on search engines to crawl the web. The French National Library selects websites to be archived based on a list of domain names delivered by French operators Afnic (managing French country code top-level domain names) and OVH (providing hosting and domain name registration), and complete their collections around events and topics selected by the curators.

The existing techno-legal arsenal to delete

52 Currently, there seem to be no reason to believe that the RTBF will affect web archiving. Beyond RTBF and the right to de-indexation however, web archiving is subjected to other laws and users' requests, which can already effectively remove content. For example, the British Library implemented a Notice and Take Down policy to assess requests to remove content or stop making it available. Their website provides the following explanation on their practices:

Valid reasons for withdrawing or removing material include, but are not limited to:
 Agreements for embargoing access
 Court injunctions
 Legal requirements
 Proven violations of copyright or database right, not covered by legal deposit legislation or a limitation or exception in UK copyright law

Material that has been found to be libellous or defamatory
Breaches of confidentiality.

- 53 Another example is the Wayback machine robot, which follows links and preserves webpages it can find. In principle, it is very easy to opt out from archiving, just by adding a robots.txt file to stop the crawler and ask previous content to be removed.
- 54 These practices lead us to believe that the *Google Spain* ruling will have little effect upon archiving, as there are already procedures in place to have content removed from the archives on request without judicial proceeding. Practices will evolve even without legal requirements, and it will be interesting to see which strategies and techniques archives adopt concerning personal information held in the records. On that note, the former British Library Head of web archiving makes the following remark:
- The Google case does not significantly change our current notice and take-down policy for non-print Legal Deposit material. However, we will review our practice and procedures to reflect the judgement, especially with regard to indexing, cataloguing and resource discovery based on individuals' names." (Hockx-Yu, 2014).
- 55 However, as section 3.4 will discuss in more detail, the RTBF will be built into legislation as a new right to erasure contained in the General Data Protection Regulation, which will come into effect in 2016, and which will end-up going much further than the existing version of the RTBF contained in *Google Spain*. As discussed, there is currently no evidence to indicate that web archives are being affected by the RTBF, as they are already required to remove links to content. With the enactment of the General Data Protection Regulation it may be possible to foresee a future in which web archives will be required to perform actions that are more cumbersome than those already in existence. However, this is speculation, and we will need to wait and see.
- 56 Web archives may have more reasons for concern in other de-listing and blocking practices, namely copyright, data materiality and mistakes. These include: "Findings outline the challenges that still face researchers who wish to engage seriously with web content as an object of research, and archivists who must strike a balance reflecting a range of user needs." (Dougherty & Meyer, 2014).
- 57 Copyright may prevent the preservation of digital native content in jurisdictions that do not have a legal deposit law and/or an exception to copyright for libraries (Dulong de Rosnay & Musiani, 2012). Legal deposit laws indeed do not trump copyright on digital native content that can be consulted only on the premises of the libraries. Besides archiving, content collected by means of legal deposit is not made available online, to the public or to search engines. The consultation of content collected through legal deposit, whose reproduction is authorized on the basis of the legal deposit of the press, which is part of heritage law and not of copyright law, is available on the premises only for consultation by accredited researchers. The British Library Head of web archiving recalls that "websites archived for Legal Deposit are only accessible within the Legal Deposit Libraries' reading rooms and the content of the archive is not available for search engines (Hockx-Yu, 2014). According to French law for legal deposit ¹², authors cannot prevent authorized organisms (the national library) to reproduce their work for the purpose of preservation and onsite consultation by accredited researchers for their usage only; but this does not cover online publication. Similarly, the Twitter archive at the Library of Congress is not open for research.

Right to erasure, right to remember

58 While the RTBF was originated from the interpretation given to the existing law by the CJEU in 2014, a 2016 development is about to move the debate forward considerably. The aforementioned General Data Protection Regulation (GDPR), which comes into force in 2016, repeals the Data Protection Directive and establishes an updated regime geared towards the digital age. One of the biggest changes present in the Regulation is that it consolidates the various rights and principles from the existing Directive that were dealing with outdated and/or erroneous data, and puts them together into a new full-fledged right, the “right to erasure.” Article 17 of the GDPR will create an obligation for Member States to provide data subjects with the right to obtain from the controller erasure of personal data where one of various requirements contained in Articles 5 and 6 have not been met. Some of these requirements relevant for the existing article are:

The data is no longer necessary in relation to the purposes for which it was collected or processed.

The data subject has withdrawn his consent.

The data subject objects to the processing and there is no legitimate grounds to deny this request.

The data has been processed unlawfully.

59 There is a glaring omission to the above, and it is the existing requirement that data “must be accurate and kept up to date.” While the proposed right to erase gives some more power to the user to object processing, the very founding principle behind *Google Spain* is no longer relevant. In some ways, this makes the right to erase very different from the RTBF version.

60 Furthermore, Article 17 contains an inbuilt reference to balance with freedom of expression, paragraph 3 has an exception to the right to erase for the purpose of “exercising the right of freedom of expression and information.” This should hopefully lay to rest most of the criticism mentioned which see the RTBF as a possible threat to freedom of expression.

61 The main issue to understand when it comes to archiving is that the RTBF does not undermine the original content directly; it only requires that a search engine should remove the link to the content.

62 Indicative of this type of thinking is the use of the term “right to remember” (Lee, 2014). As previously stated, this is a concept that does not have any legal basis, and it is used mostly as a rhetorical device. Opponents usually support this argument by highlighting and publicizing cases where links were removed undeservedly, and then they make an argument on behalf of the public’s right to know, freedom of speech, or in this case, a non-existent right to remember.

63 The Regulation has an even more important exception for the purposes of web archiving. Article 17(3)(d) states that there will not be a right to erase “for archiving purposes in the public interest, or scientific and historical research purposes or statistical purposes,” given that the right to erase is likely to “render impossible or seriously impair the achievement of the objectives of the archiving purposes in the public interest, or the scientific and historical research purposes or the statistical purposes.”

64 Thus, while the above is not a full exception for archiving purposes, it safeguards archiving from most potentially problematic effects of the right to erase. So any erasure

that would impair archiving cannot be granted. However, this will be a question of evidence: archives will have to give proof that an exercise of the right to erase will hinder archiving, and that these purposes are in the public interest. Conversely, it is still possible that the right to erase would apply to an archive if it cannot be proven that the erasure affects the public interest. In this regard, there may still be room for concern for archivists. The International Holocaust Remembrance Alliance has complained, in this respect, that the language of the GDPR is imprecise and could lead, if left to the interpretation of individual archivists, archives to restrict access to sources, while they should remain “in full and open access”.

- 65 The ruling is not a real RTBF with “erasure” from the controller and “abstention from further dissemination” as considered in the 2011 draft proposal of General Data Protection Regulation and the 1995 Directive. Both texts are defining personal data broadly as “any information related to an identified or an identifiable person,” thus possibly including re-identification of persons after data anonymisation or involuntary traces, through linkability. This proposal of erasure caused anxiety in the archivist professions.
- 66 In the recent history of the drafting of the GDPR, there has been relatively little commentary from archives and memory institutions. Whether this is because archives do not see a threat from RTBF as such, or because they have been satisfied with the proposed changes contained in the 2016 Regulation, is unclear. In one notable example, the Association of French Archivists (*Association des Archivistes Français*), asked in 2013 for the EU not to “forbid data preservation”, as they considered that the GDPR would contain rules that would make it an obligation for archives to destroy or anonymise the data. These concerns did not materialise. Furthermore, at the time they were criticised by Jan-Philipp Albrecht, a German member of the European Parliament, as “a little bit exaggerated and misleading” (Pfanner, 2013).
- 67 A recent press communication on the GDPR reveals another issue: the above-mentioned International Holocaust Remembrance Alliance advocates to member states of the EU to “take all necessary steps to facilitate the opening of archives in order to ensure that all documents bearing on the Holocaust are available to researchers.” They comment that while the GDPR would contain some exceptions for historical research, they were concerned about the imprecision of the language. The same concern to find the truth and never forget has been expressed in relation with the search for truth in Latin America: “the content of this “right” notwithstanding, the name itself was an affront to Latin America; rather than promoting this type of erasure, we have spent the past few decades in search of the truth regarding what occurred during the dark years of the military dictatorships.” (Bertoni, 2015).
- 68 However, even if the language of the Regulation is clear enough to allow a right to remember, we will undoubtedly need guidelines from national data protection regulators to ensure that historical archives are not negatively affected. For the time being, the ambiguity present in the RTBF *Google Spain* ruling is about to disappear.

Conclusion: Forget and delete, Privacy-by-Design for web archiving

- 69 While the right to be forgotten has been interpreted as a potential threat to freedom of expression, memory and web archiving, the intended application of the right to be forgotten has been limited in scope, at least as far as one can discern from the limited information available through Google's transparency report. Besides, web archiving professionals are already deleting instances on request, and other legal frameworks, namely copyright, are more likely to generate memory holes than RTBF. However, the entry into force of the General Data Protection Regulation should put most of the debate to rest, the presence of exceptions to the right to erase for both freedom of expression and archiving in the public interest serving to make potentially damaging disruption much more difficult. Future work in this area may explore wider issues.
- 70 First, the right to forget may rely on broader foundations than data protection. The threat to individual's privacy created by mass-surveillance and big data gathering and processing, by both public and private players, has become one of the most important subjects of our time (Schneier, 2015). As a response to algorithmic governance, some commentators ask for some form of right to delete (Mayer-Schönberger, 2009; Rouvroy, 2008). The object of such a right is not to hinder preservation and memory, it is to limit the effect of data mining and data analysis and restore balance in the power relation between surveillance and other marketing information systems and individuals (Szekely, 2014). Besides, research in ethics, psychology and other fields, link some form of right to be forgotten to victims' right of information self-determination and the (re)construction of identity and personality requiring underlying rights¹³.
- 71 Second, the question is broader than a binary choice between disclose (and preserve) or delete, and there can be technical solutions to manage level of publicity. There can be circles of divulgation: family, work, medical services (Szekely, 2012). Privacy Enhancing Technologies (PETs), more recently labelled Privacy-by-Design solutions, are developing "contextual approaches" (Nissenbaum, 2011). User-centric identity management systems (PRIME and PrimeLife cited by Szekely, 2012) propose to implement laws and preferences, and crawl the web to delete photos after a specific time. Thus, the question would be not to rely on legal tools, but on the technical implementation and feasibility of an actual and real RTBF, which would remove all instances of the resource and make it impossible to access, reproduce and disseminate them.
- 72 In the same vein, engineers and computer scientists are leading further work on Digital Rights Management (DRM), which had been devised to control the unauthorised flow of music on peer-to-peer networks. Removing content because of copyright or because of privacy leads to the same act. Access control measures may be used try to implement the RTBF and erasure, using semantic web and linked data web standards. This would be a paradox, since these protocols were developed to share content, rather than to implement conditional access restrictions and manage consent (O'Hara, 2012; Kasioumis et al, 2014). The standards of the preservation activities such as PREMIS, METS and the standards developed by the copyright industry (Dulong de Rosnay, 2007, 2016) remain available. MPEG-21 ISO Digital Item Declaration, an access control standard adopted in 2003 and revised in 2005, has been revised for and adapted to the RTBF in 2014: "enforcement of 'digital forgetting' is implemented over an information-centric model

for the Internet. The defined solution enables the definitive elimination of digital objects, either on-demand or on a pre-scheduled basis, and, hence, their 'forgetting.'" (Almeida et al, 2014).

- 73 Digital golems¹⁴ (Dulong de Rosnay, 2016), machines implementing actions automatically – encoding rules into technical specifications, being Digital Rights Management systems (DRM) for copyright, or a Privacy-by-Design digital forgetting instrument which would be implementing a RTBF – are not part of a dystopian future. They are an illustration of the conflict between regulation by technology and regulation by law, between a possibility to preserve and a right to oblivion.

BIBLIOGRAPHY

- ALMEIDA Fernando, CASTRO Helder, ANDRADE Maria T., TROPEA Giuseppe, BLEFARI Melazzi Nicola, SIGNORELLO Salvatore, MOUSAS Aziz, ANADIOTIS Angelos, KAKLAMANI Dimitra, VENIERIS Iakovos, MINELLI Sam & DIFINO Angelo (2014). "Digital forgetting in information-centric networks - the CONVERGENCE perspective", *New Review of Hypermedia and Multimedia*, 20 (2), pp. 169-187.
- AMBROSE Meg Leta (2013). "It's about time: privacy, information life cycles, and the right to be forgotten", *Stanford Technology Law Review*, 16 (2), , pp. 369-422.
- BRÜGGER Niels (2011). "Web Archiving – Between Past, Present, and Future", in Consalvo Mía & Ess Charles (eds), *The Handbook of Internet Studies*, Oxford, Wiley-Blackwell, pp. 24-42.
- BRÜGGER Niels (2012). "Web History and the Web as a Historical Source", *Zeithistorische Forschungen/Studies in Contemporary History*, 9 (2), pp. 316-325.
- BIGNAMI Francesca (2008). "The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts", *Cornell International Law Journal*, 41 (2), pp. 211-249.
- BYGRAVE Lee A. (2002). *Data protection law: approaching its rationale, logic and limits*, Amsterdam, Kluwer Law Intl.
- CHARLESWORTH Andrew (2000). "Clash of the data titans? US and EU data privacy regulation", *European Public Law*, 6 (2), pp. 253-274.
- de TERWAGNE Cécile (2014). "The Right to be Forgotten and Informational Autonomy in the Digital Environment", in Ghezzi Alessia, Pereira Ângela & Vesnic-Alujevic Lucia (ed.), *The ethics of memory in a digital age: interrogating the right to be forgotten*, Basingstoke, Palgrave Macmillan, pp. 82-100.
- DOUGHERTY Meghan & MEYER Eric T. (2014), "Community, tools, and practices in web archiving: The state-of-the-art in relation to social science and humanities research needs", *Journal of the Association for Information Science and Technology*, 65, pp. 2195–2209.
- DULONG de ROSNAY Mélanie (2007). « La mise à disposition des œuvres et des informations sur les réseaux : régulation juridique et régulation technique », thèse de droit, Université Panthéon-Assas Paris II.

- DULONG de ROSNAY Mélanie & MUSIANI Francesca (2012). "The Preservation of Digital Heritage: Epistemological and Legal Reflections", *ESSACHESS - Journal for Communication Studies*, 5 (2), pp. 81-94.
- DULONG de ROSNAY Mélanie (2016). *Les golems du numérique. Droit d'Auteur et Lex Electronica (Digital Golems. Copyright and Lex Electronica)*, Paris, Presses des Mines.
- FAZLIOGLU Muge (2013). "Forget me not: the clash of the right to be forgotten and freedom of expression on the Internet", *International Data Privacy Law*, 3 (3), pp. 149-157.
- JEFFREY Stuart (2012). "A new Digital Dark Age? Collaborative web tools, social media and long-term preservation", *World Archaeology*, 44 (4), pp. 553-570.
- KASIOUMIS Nikos, BANOS Vangelis & KALB Hendrik (2014). Towards building a blog preservation platform, *World Wide Web Journal*, 17 (4), pp. 799-825.
- KOOPS Bert-Jaap (2011). "Forgetting footprints, shunning shadows: A critical analysis of the 'right to be forgotten' in big data practice", *SCRIPTed*, 8 (3), pp. 229-256.
- MASANES Julien (2002). "Towards Continuous Web Archiving. First Results and an Agenda for the Future". *D-Lib Magazine*, 8 (1), [online], accessed 17.10.2016. URL: <http://www.dlib.org/dlib/december02/masan/12masanes.html>.
- MATTHIESSON Sophie (2010). "Who's Afraid of the Limelight? The Trafigura and Terry Super-Injunctions, and the Subsequent Fallout". *Journal of Media Law*, 2 (2), pp. 153-167.
- MAYER-SCHÖNBERGER Victor (2009). *Delete. The Virtue of Forgetting in the Digital Age*, Princeton, NJ, Princeton University Press.
- NISSENBAUM Helen (2011). "A Contextual Approach to Privacy Online", *Daedalus, the Journal of the American Academy of Arts & Sciences*, 140 (4), pp. 32-48.
- O'HARA Kieron (2012). "Can Semantic Web Technology Help Implement a Right to Be Forgotten?", *Computers and Law*, 22 (6), pp. 1-5.
- PARMAR Maya (2014). "Memorialising 40 years since Idi Amin's expulsion: Digital 'memory mania' to the 'right to be forgotten'", *South Asian Popular Culture*, 12 (1), pp. 1-14.
- ROUVROY Antoinette (2008). « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? » in Lacour Stéphanie (ed.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*, Paris, L'Harmattan, pp. 249-278.
- ROSEN Jeffrey (2012). "The right to be forgotten", *Stanford Law Review Online*, 64, pp. 88-92.
- SCHNEIER Bruce (2015). *Data and Goliath: the hidden battles to collect your data and control your world*, New York, NY, W. W. Norton & Company.
- SZEKELY Ivan (2012). "The right to forget, the right to be forgotten", in Gutwirth Serge, Leenes Ronald, De Hert Paul & Pouillet Yves (eds.), *European Data Protection: In Good Health?*, New York, Springer, pp. 347-363.
- SZEKELY Ivan (2014). "The Right to be Forgotten and the New Archival Paradigm", in Pereira Ângela, Ghezzi Alessia & Vesnic-Alujevic Lucia (eds.), *The ethics of memory in a digital age: interrogating the right to be forgotten*, Basingstoke, Palgrave Macmillan, pp. 28-49.
- TAMBINI Damian, LEONARDI Danilo & MARSDEN Chris T. (2008). *Codifying cyberspace: communications self-regulation in the age of Internet convergence*, Oxford, Routledge.
- TEMKIN Jennifer (2003). *Rape and the Legal Process* (2nd Edition), Oxford, Oxford University Press.

URBAN Jennifer & QUILTER Laura (2006). "Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act", *Santa Clara Computer and High Technology Law Journal*, 22, pp. 621-693.

WERRO Franz (2009). "The right to inform v. the right to be forgotten: A transatlantic clash", in Colombi Ciacchi Aurelia, Godt Christine, Rott Peter & Smith Leslie Jane (eds.), *Liability in the Third Millennium*, Baden-Baden, Nomos Verlag, pp. 285-300.

Legal references and cases

Abbey v Gilligan [2012] EWHC.

Campbell v MGN Ltd [2004] UKHL 22.

Davydiuk v. Internet Archive Canada, 2014 FC 944 (CanLII).

DPD. 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. OJ L 281, 23.11.1995, p. 31-50.

GDPR. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 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), OJ L 119, 4.5.2016, p. 1-88.

Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311.

Google Spain. *Google Spain v Agencia Española de Protección de Datos and Mario Costeja González case* (C131/12), Court of Justice of the European Union (CJEU), 13.05.2014. ECLI:EU:C:2014:317.

Jääskinen. Opinion of Advocate General Jääskinen, Case C-131/12 Google Spain SL Google Inc. v Agencia Española de Protección de Datos (AEPD) Mario Costeja González. Reference for a preliminary ruling from the Audiencia Nacional (Spain), *Curia*, 25.06.2013.

Murray v Express Newspapers Ltd [2007] EWHC 1980 (Ch).

OBG Ltd v Allan and Douglas v Hello! (2008) 1 AC 1.

Schrems. Maximilian Schrems v Data Protection Commissioner (C362/14), Court of Justice of the European Union (CJEU). 06.10.2015. ECLI:EU:C:2015:650.

Vidal -Hall & Ors v Google Inc [2014] EWHC 13 (QB).

Wainwright v Home Office [2003] UKHL 53.

Online references (all URLs last accessed on 27.05.2016)

Association des archivistes français, Adjourn the adoption of the regulation about personal data, Change.org. <https://www.change.org/p/the-european-parliament-adjourn-the-adoption-of-the-regulation-about-personal-data>

BALKAM Stephen, The Right to Remember, *Huffington Post*, 16.05.2014.

http://www.huffingtonpost.com/stephen-balkam/the-right-to-remember_b_5338223.html

BERTONI Eduardo, The Right to Be Forgotten: An Insult to Latin American History, *Huffington Post*, 24.09.2014. <http://huff.to/1GMfjot>

BRIGHAM Geoff & PAULSON Michelle, Wikipedia pages censored in European search results, 06.08.2014. <https://blog.wikimedia.org/2014/08/06/wikipedia-pages-censored-in-european-search-results/>

British Library. Notice and Takedown. <http://www.bl.uk/aboutus/legaldeposit/complaints/noticetakedown/>

CURTIS Sophie, PHILIPSON Alice, Wikipedia founder: EU's Right to be Forgotten is 'deeply immoral', *The Telegraph*, 06.08.2014. <http://www.telegraph.co.uk/technology/wikipedia/11015901/EU-ruling-on-link-removal-deeply-immoral-says-Wikipedia-founder.html>

Day of Archaeology. <http://www.dayofarchaeology.com/>

Google transparency report for European privacy requests for search removals, Data last updated: 15.12.2014. <https://www.google.com/transparencyreport/removals/europeprivacy/>

GUADAMUZ Andrés, You Have the Right to Be Forgotten, *Technollama Blog*, 19.05.2014. <http://www.technollama.co.uk/you-have-the-right-to-be-forgotten>

HOCKX-YU Helen. A right to be remembered. *UK Web Archive blog, British Library*, 21.07.2014. <http://britishlibrary.typepad.co.uk/webarchive/2014/07/a-right-to-be-remembered.html>

HOLE Jackie, Do You Have the Right To Be Forgotten?, *State of Digital*, 03.06.2014. <http://www.stateofdigital.com/right-to-be-forgotten/>

International Holocaust Remembrance Alliance. General Data Protection Regulation, 25.06.2015. <https://www.holocaustremembrance.com/media-room/stories/general-data-protection-regulation>

LEE Dave, BBC to publish 'right to be forgotten' removals list, *BBC News*, 17.10.2014. <http://www.bbc.co.uk/news/technology-29658085>

LEPORE Jill, The Cobweb. Can the Internet be archived? *The New Yorker. Annals of Technology*, 26.01.2015. <http://www.newyorker.com/magazine/2015/01/26/cobweb>

LEVINE David, The MH17 Disaster Demonstrates the Dangers of "Right to Be Forgotten", *Slate Future Tense*, 17.07.2014. http://www.slate.com/blogs/future_tense/2014/07/22/mh17_investigation_and_the_right_to_be_forgotten.html

LYONS David, Right to be forgotten? Forget about it. *TechPolicyDaily.com*. 22.05.2014. <http://www.techpolicydaily.com/technology/right-forgotten-forget/>

Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data. 13.05.2015. <https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd#.mxjhd34sh>

SOLON Olivia, People have the right to be forgotten, rules EU court, *Wired UK*, 13.05.2014. <http://www.wired.co.uk/article/right-to-be-forgotten-blog>

PFANNER Eric, Archivists in France Fight a Privacy Initiative. *New York Times*, 17.06.2013. <http://www.nytimes.com/2013/06/17/technology/archivists-in-france-push-against-privacy-movement.html>

POWLES, Julia and LARSEN, Rebekah (compilers), Academic Commentary: Google Spain. <http://www.cambridge-code.org/googlespain.html>

SPAUWEN Joran, van den BRINK Jens, Dutch Google Spain ruling: More Freedom of Speech, Less Right to Be Forgotten for Criminals, *Inform's Blog*, 27.09.2014. <https://inform.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/#more-27910>

STOBBE Richard, Copyright Implications of a “Right to be Forgotten”? Or How to Take-Down the Internet Archive. *IPBlog.ca*, 04.12.2014. <http://www.lexology.com/library/detail.aspx?g=698e6429-03e3-4da3-acbd-1b2ca1b8831f>

TRÉGUER Félix, Right to Be Forgotten: With Free Expression Under Threat, Europe Needs a ‘Marco Civil Moment’. *Global Voices*, 09.11.2014. <https://globalvoices.org/2014/09/11/right-to-be-forgotten-with-free-expression-under-threat-europe-needs-a-marco-civil-moment/>

TRETIKOV Lila, European court decision punches holes in free knowledge, 06.08.2014. <http://blog.wikimedia.org/2014/08/06/european-court-decision-punches-holes-in-free-knowledge/>

Wikipedia, Notices received from search engines. https://wikimediafoundation.org/wiki/Notices_received_from_search_engines

Wikipedia, Temptation Island. https://nl.wikipedia.org/wiki/Temptation_Island.

Wikipedia, Helen Duval. https://nl.wikipedia.org/wiki/Helen_Duval.

Wikipedia, Gerry Hutch. https://en.wikipedia.org/wiki/Gerry_Hutch.

Wikipedia, Nadia Almada. https://en.wikipedia.org/wiki/Nadia_Almada.

ZIMMERMANN Jérémie, la Parisienne Libérée, Rien à cacher, (English, Spanish, Hungarian subtitles). YouTube, 06.02.2014. <https://www.youtube.com/watch?v=rEwf4sDgxHo&feature=youtu.be>

ZITTRAIN Jonathan, Don’t Force Google to “Forget”, *The New York Times*, 14.05.2014. <http://nrs.harvard.edu/urn-3:HUL.InstRepos:12921731>

NOTES

1. <https://blog.wikimedia.org/2016/10/19/petition-right-to-be-forgotten/>
2. https://en.wikipedia.org/wiki/Commission_nationale_de_l%27informatique_et_des_libert%C3%A9s
3. Information self-determination is the right to control and determine the usage made of one’s personal information.
4. *OBG Ltd v Allan and Douglas v Hello!* (2008) 1 Appeals Court 1.
5. *Campbell v MGN Ltd* [2004] UK House of Lords 22.
6. Amongst other, *Murray v Express Newspapers Ltd* [2007] England and Wales High Court 1980 (Chancery Division); *Abbey v Gilligan* [2012] England and Wales High Court; and *Vidal-Hall & Others v Google Inc* [2014] England and Wales High Court 13 (Queen’s Bench Division).
7. *Wainwright v Home Office* [2003] UK House of Lords 53.
8. *Google Inc v Vidal-Hall & Others* [2015] England and Wales Court of Appeals Civil 311.
9. This section contains commentary previously published in (Guadamuz, 2014).
10. A technical act performed either by a search engine as in the case of the Google Spain case, or by a web archiving crawler.
11. The Advocate General provides an opinion before the decision, the court can decide to follow it, rely on it, or ignore it (Jääskinen, 2013).
12. Code du patrimoine Article L132-4. Modifié par la loi n°2006-961 du 1 août 2006 - art. 42 JORF 3 août 2006
13. “Recommendation on the microfilm recording of documents containing personal data relating to the persecution of Jews during the Nazi period, and on their transfer to the Yad Vashem Archives in Jerusalem”. In The first three years of the Parliamentary Commissioner for Data Protection and Freedom of Information, edited by László Majtényi. Budapest: Office of the

Parliamentary Commissioner for Data Protection and Freedom of Information, 1998. – An analysis of conflicts between the legitimate purposes of unveiling historical events and the privacy rights of the victims of history. Cited by Szekely Ivan (2012).

14. This mythological creature is applying orders, can be invisible, even deactivated for Sabbath, and without control, can turn out to be dangerous even for their masters.

ABSTRACTS

This article studies the possible impact of the “right to be forgotten” (RTBF) on the preservation of native digital heritage. It analyses the extent to which archival practices may be affected by the new right, and whether the web may become impossible to preserve for future generations, risking to disappear from memories and history since no version would be available in public or private archives. Collective rights to remember and to memory, free access to information and freedom of expression, seem to clash with private individuals’ right to privacy. After a presentation of core legal concepts of privacy, data protection and freedom of expression, we analyse the case of the European Union Court of Justice vs. Google concerning the right to be forgotten, and look deeper into the controversies generated by the decision. We conclude that there is no room for concern for archives and for the right to remember given the restricted application of RTBF.

Cet article étudie l’impact possible du « droit à l’oubli » (RTBF) sur la préservation du patrimoine numérique natif. Il analyse si les pratiques d’archivage sont susceptibles d’être affectées par le nouveau droit et s’il pourrait devenir impossible de préserver le Web pour les générations futures, avec le risque pour certains contenus de disparaître de la mémoire et de l’histoire si aucune version n’était disponible dans les archives publiques ou privées. Le droit collectif au souvenir et à la mémoire, l’accès libre à l’information et la liberté d’expression semblent entrer en conflit avec les droits individuels à la vie privée. Après une présentation des concepts juridiques fondamentaux de la vie privée, de la protection des données personnelles et de la liberté d’expression, nous analysons l’arrêt Google de la Cour de Justice de l’Union Européenne et le droit à l’oubli, et examinons les controverses qui ont été générées par la décision. On conclut que les archives et le droit au souvenir ne seront pas affectés par le droit à l’oubli, étant donné son application restreinte.

INDEX

Mots-clés: données personnelles, archives numérique, archivage du Web, droit à l’oubli, mémoire, vie privée, droit au souvenir, Google, Wikipedia

Keywords: data protection, digital archives, web archives, right to be forgotten, memory, privacy, right to remember

AUTHORS

MELANIE DULONG DE ROSNAY

CNRS/Paris-Sorbonne/UPMC, Institute of Communication Sciences

ANDRES GUADAMUZ

University of Sussex, School of Law, Politics and Sociology