Hammering Square Pegs into Round Holes: The Geographical Scope of Application of the EU Right to be Delisted

REYMOND, Michel

Abstract

On May 13, 2014, the European Court of Justice decided, in the case of Google Spain, that search engines are bound to remove, upon request, results pointing to websites holding “inadequate, irrelevant, or excessive” information about European citizens, thus granting the latter a so-called ‘Right to be Forgotten,’ or more precisely a ‘Right to be Delisted.’ In the case at hand, it was found that European principles of data protection applied to Google’s search engine business through the presence of Google Spain, a locally-focused advertising management office established in Madrid. Left unexplored, however, was the question of whether other foreign search engines that have fewer contacts with the legal order of the European Union, such as Duck Duck Go, also fall under its scope. With this interrogation over the extraterritorial application of EU data protection law as a starting point, the paper confronts, through the use of a private international law inspired methodology, the scope rules of Directive 95/46/EC on data protection against hypothetical cases involving search result delisting requests. Through […]

Reference


Available at: http://archive-ouverte.unige.ch/unige:87992

Disclaimer: layout of this document may differ from the published version.
Hammering Square Pegs into Round Holes: 
The Geographical Scope of Application of the EU Right to be Delisted 

Dr. Michel J. Reymond 

This paper can be downloaded without charge at: 

The Berkman Klein Center for Internet & Society Research Publication Series:  
https://cyber.harvard.edu/publications/2016/squarepegs 

The Social Science Research Network Electronic Paper Collection:  
http://ssrn.com/abstract=2838872
Hammering Square Pegs into Round Holes

The Geographical Scope of Application of the EU Right to be Delisted

Dr. Michel J. Reymond
Visiting Researcher
Berkman Klein Center
for Internet & Society
at Harvard University
HAMMERING SQUARE PEGS INTO ROUND HOLES:
THE GEOGRAPHICAL SCOPE OF APPLICATION OF THE EU RIGHT TO BE DELISTED

DR. MICHEL J. REYMOND

Dr. Michel J. Reymond is a visiting researcher at the Berkman Klein Center for Internet & Society at Harvard University for the 2015-2016 academic year under funding from the Swiss National Science Foundation. With a background in private international law and comparative law, his work is mainly centered on the relationship between regulation, competing legal orders, and the Internet. Serving as a research assistant at his home institution, the University of Geneva, Michel J. Reymond is also dedicated to teaching and has notably coached local students for the Vienna Moot Court Competition.
ABSTRACT

On May 13, 2014, the European Court of Justice decided, in the case of Google Spain, that search engines are bound to remove, upon request, results pointing to websites holding “inadequate, irrelevant, or excessive” information about European citizens, thus granting the latter a so-called ‘Right to be Forgotten,’ or more precisely a ‘Right to be Delisted.’ In the case at hand, it was found that European principles of data protection applied to Google’s search engine business through the presence of Google Spain, a locally-focused advertising management office established in Madrid. Left unexplored, however, was the question of whether other foreign search engines that have fewer contacts with the legal order of the European Union, such as Duck Duck Go, also fall under its scope.

With this interrogation over the extraterritorial application of EU data protection law as a starting point, the paper confronts, through the use of a private international law inspired methodology, the scope rules of Directive 95/46/EC on data protection against hypothetical cases involving search result delisting requests. Through the results so obtained, it highlights that, due to a rift between the individual, personality focused nature of the Right to be Delisted and the processing, data controller oriented nature of the scope rules of the Directive, answering these questions remains a convoluted and inconsistent process akin to hammering square pegs into round holes. It concludes by proposing solutions, both de lege lata and de lege ferenda, which may inspire further developments.
**TABLE OF CONTENTS**

*Introduction* .................................................................................................................. 1

The Data Protection Directive ......................................................................................... 4

The ECJ’s Google Spain decision .................................................................................. 5

Current implementation model ...................................................................................... 8

*Defining the geographical scope of the Right to be Delisted* ...................................... 10

*Jurisdiction* .................................................................................................................. 12

DPA jurisdiction over a foreign search engine ............................................................... 12

  Article 28 (4) of the Data Protection Directive........................................................... 12
  Definition of data processing ....................................................................................... 15
  Data processing operations targeted by the Right to be Delisted ............................... 16
  Processing operations involved in search engine activity ............................................. 18
  Locating the place of processing ................................................................................ 20
  Place of crawling .......................................................................................................... 20
  Place of indexing and ranking ...................................................................................... 21
  Place of display ............................................................................................................. 21
  Application to the example cases ................................................................................ 22

Limiting factor: the claimant’s links with the European Union .................................... 23

  Standard ....................................................................................................................... 23
  Application to the example cases ................................................................................ 24

*Applicable law* .............................................................................................................. 25

Article 4 (1) of the Data Protection Directive ............................................................... 25

Letter (a): the law of the establishment of the data controller ......................................... 26

  Data processing ........................................................................................................... 26
  Establishment .............................................................................................................. 26
  Processing performed in the context of the activities of an establishment .................... 28
    Google Spain and the ‘context of activities’ ................................................................ 29
    Multiple establishments .......................................................................................... 32
  Application to the example cases ................................................................................ 33

Letter (c): the law of the place where processing equipment is located .......................... 34

  Standard ....................................................................................................................... 34
  Application to the example cases ................................................................................ 36

*Comments and analysis* ............................................................................................... 37

Complexity, obscurity and inconsistency ..................................................................... 37

Square pegs and round holes: the Right to be Delisted v. the Data Protection Directive .... 39

Google Spain revisited: the Right to be Delisted as a destination-based personality harm... 41
Proposals ................................................................................................................................... 43

Jurisdiction .................................................................................................................................. 44

Applicable law................................................................................................................................ 44

Conclusion ...................................................................................................................................... 46
ACKNOWLEDGEMENTS

The present work is part of the author’s postdoctoral research on the topic of the Right to be Forgotten in private international law, performed during the academic year of 2015-2016 under funding from the Swiss National Science Foundation. He would like to thank Prof. Jacques De Werra, Prof. Thomas Kadner Graziano and Prof. Gian Paolo Romano, along with his colleagues at the University of Geneva, for the support they have provided to this project. The present work also owes much to the fellows, affiliates, and staff members of the Berkman Klein Center for Internet & Society with whom the author has had the privilege of sharing many discussions during the past year; in particular, Christopher T. Bavitz, Charlie Ruth Castro, David O’Brien, Jason Griffey, Eldar Haber, Adam Holland, Tiffany Lin, Patrick Murck, and Amy Aixi Zhang have been instrumental, both by their insights and their companionship, to the drafting process.
INTRODUCTION

On May 13, 2014, the European Court of Justice (‘ECJ’) rendered the Google Spain decision, in which it declared that the principles of European data protection law contained in Directive 95/46/EC applied directly to search engine operators and imposed on them the obligation to implement a so-called ‘Right to be Forgotten’. This obligation, which came to become more correctly identified as a ‘Right to be Delisted’ (‘RTBD’), allows European citizens to request that all search engines remove results pointing to “outdated, irrelevant or excessive” information harming the privacy rights granted to them by the Directive along with articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Google Spain is also indicative of a more general trend, followed by the European Union legislature and spurred by the emergence of the digital economy, leading towards a stronger protection of the fundamental personal rights conferred upon physical persons, or so-called ‘data subjects’, and exercised against entities making use of their data for their own purposes. In that sense, the decision is a stepping stone of sorts leading the way towards entry into force of the General Data Protection Regulation (‘GDPR’), an instrument slated to replace the Directive in 2018, and effectively creating a unified legal system of data protection across the territory of the European Union. Article 17 of this document envisages the creation of a ‘Right to be Forgotten’ which may go above and beyond the scope of Google Spain’s RTBD.

---

2 European Court of Justice, Google Spain SL v. AEPD, Case C-131/12, May 13 2014.
3 Julia Powles, The Case That Won’t Be Forgotten, 47 Loy. U. Chi. L.J. 583, 584 (2015), at note 2 (“The right is misnamed because the right endorsed by the ruling is far narrower, legally and practically, than anything approximating “forgetting”. Properly, the case concerns data erasure, correction, and obscurity.”).
4 As one of the main points of analysis proposed in the present article lies in the definition of the circle of beneficiaries of the RTBD, the term ‘European citizens’ should here be understood as a simplified shorthand used for the purposes of this introductory section. See infra, at 23-25.
5 Google Spain, Case C-131/12, at pars. 95-99.
6 Regulation (EU) 2016/679 of the European Parliament and of the Council 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), Official Journal of the European Union, L 119/1, May 4, 2016. It is slated to enter into force in two years following the date of its publication in the Official Journal.
7 Article 17 of the GDPR provides a “right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data” in several cases. The exact implications of the provision are, however, heavily debated. Some scholars have argued that it mainly restates data protection rights already present under the Directive; see Jean-Michel Bruguère, Le “droit à” l’oubli numérique, un droit à oublier, 2014 D. 299; Oleksandr Pastukhov, The right to oblivion: what’s in a name?, 19 C.T.L.R. 14 (2014); Eduardo Ustaran, EU: The wider effects of the Google ‘right to be forgotten’ case, P. & D.P., Sept. 2014, at 8-9; Brendan van Alsenoy, Aleksandra Kucznerawy & Jeff Ausloos, Search engines after Google Spain: internet@liberty or privacy@peril?, ICRI Working Paper 15/2013, Sept. 6, 2013, at 42-44. Others authors have however opined that the article expands the current regime to grant an extended right for data subjects to request the deletion of all kinds of personal data; in this sense, see Monika Kushewsky, The right to be forgotten – the fog finally lifts, P. & D.P., Jan./Feb. 2012, at 10; Jeffrey Rosen, The Right to Be Forgotten, 54 Stan. L. Rev. Online 88 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten; Michael Rustad & Sanna Kulevska, Reconceptualizing the Right to Be Forgotten to Enable Transatlantic Data Flow, 28 Harvard Journal of Law and Technology 349, 367-376. Highlighting that the provision itself does not provide any guidance on that point and that it may be interpreted in both of these ways, see Daphne Keller, The Final Draft of Europe’s “Right to be Forgotten” Law, The Center for Internet and Society at Stanford Law School Blog (Dec. 17, 2015), http://cyberlaw.stanford.edu/blog/2015/12/final-draft-europes-right-be-forgotten-law; Patricia Sánchez Abril & Jacqueline D. Lipton, The Right to be Forgotten: Who Decides What the World Forgets?, 103 Kentucky Law Journal 363, 370-372 (2014-2015) (“The GDPR sketches only faint boundaries for the right to be forgotten.”); Meg Leta Jones, Ctrl+Z: the right to be forgotten, 47-53 (New York University Press, 2016).
Since its inception in *Google Spain*, the RTBD has revealed itself as a challenging and multifaceted concept of law. Commentators and scholars have isolated and explored a multitude of different controversial issues left in its wake. For example, one can mention the implications of taking down search results on the equilibrium between freedom of speech and the right to information against the protection of personal privacy and data protection rights; one can also point towards the debate surrounding the kind of criteria that should be used to assess whether or not a search result should be removed in a given case, and on the difficulties of formulating the RTBD as a concrete legal standard; also of note are the issues raised by its implementation model, which currently confers to search engines the main task of deciding upon each individual search result removal claim filed against it, and which sees official bodies, such as local courts and data protection authorities, only play a secondary role.

The present paper aims at offering its own piece of this overall puzzle by tackling the issue of the RTBD’s geographical scope. The basic premise is as follows: the RTBD, which is part of the principles set forth by the Data Protection Directive, is primarily directed against Google Inc.’s eponymous search engine, which is by far the leader of the Internet search market worldwide. The fact that Google, though it is headquartered in Mountain View, California and thus outside of the territory of the European Union, is nevertheless bound to implement the RTBD is hardly controversial given that it has established multiple subsidiaries located in different Member States, and that it receives more than 90% of all search queries performed by end users located there. Less clear, however, is the situation of smaller search engines, which may not have the same relationship with the legal order of the European Union.

Is a search engine, headquartered in the US and having no offices nor representatives located in Europe, bound to implement the RTBD as soon as it serves a handful of search results there? If a person living in Spain wishes to remove inappropriate search results provided by that same search engine, which by hypothesis has not implemented a form allowing her to request such a removal, then may that person file a complaint against it with her local data protection authority? Will that authority have jurisdiction to impose fines upon the American search engine if it finds that the link should be removed? What links to Spain, or the rest of the European Union for that matter, would be deemed sufficient for this search engine to be

---


9 Discussing how Google managed to monopolize the space of the RTBD, see Powles, *The Case*, supra, at 590-606.

10 Google locations, Google (last visited May 7, 2016), https://www.google.com/about/company/facts/locations/.

found obliged to comply with the RTBD? Finally, is the appreciation of these contacts foreseeable for all of the parties involved?\textsuperscript{12}

While these interrogations might seem rather theoretical at first blush, it must be pointed out that one of Google’s competitors, the Duck Duck Go search engine, fits into the profile described above due to its stature as a small startup company located in Pennsylvania.\textsuperscript{13} As such, it certainly has an interest in knowing whether or not the RTBD applies to the search results it serves. Correspondingly, physical persons located in Europe wishing to control the information that is displayed about them on that search engine also have an interest in knowing whether or not it is subject to the RTBD, and furthermore in knowing if and how they may be able to realize that right by bringing a claim against it. The interests at stake when discussing the geographical scope of the RTBD are thus quite tangible, not only because all of these actors have a need for legal certainty, but also because these situations can test whether or not the RTBD is able to function adequately as a general rule of law, potentially applicable to all search engines available on the Internet, or if it is instead an uncertain mandate made practically possible today by its reliance on Google’s current hegemony in that market.

Through a series of hypothetical cases similar to the Duck Duck Go example used above, the present paper will observe how the RTBD’s geographical scope materializes in specific situations. With the RTBD having no territorial scope rules of its own, this exercise will hinge upon the application and interpretation of the scope provisions found in its underlying legal framework, the 1995 Data Protection Directive. Through the results so obtained, it will be shown that, due to an underlying dysfunction between the way in which the Directive traditionally defines its own territorial scope of application and the nature of the RTBD as a

\textsuperscript{12} Outside of the scope of this study, yet related to the issue at hand, is the question of the geographical scope of the delisting itself, i.e. whether a search engine – once it is found that it must implement the RTBD – should remove its results only from searches emanating from users located in the European Union, or if it must scrub results on a global basis. Google had, until recently, opted for an easily circumvented top level domain based form of isolating European search results from those served in the rest of the world, meaning that a user accessing the service through http://www.google.fr or http://www.google.de would obtain a RTBD compliant list of results whereas she would have access to all of the removed items through http://www.google.com or http://www.google.com.au. Following criticism on the part of the Article 29 Data Protection Working Party – and, additionally, under the threat of fines on the part of the Commission Nationale de l’informatique et des libertés, the French national data protection authority – the company has subsequently adopted a stronger form of segmentation enforced by technical means of locating a user’s home jurisdiction; see Samuel Gibbs, \textit{Google to extend ‘right to be forgotten’ to all its domains accessed in EU}, The Guardian, (Feb. 11, 2016), http://www.theguardian.com/technology/2016/feb/11/google-extend-right-to-be-forgotten-googolecom. For more on this aspect; see, \textit{inter alia}, Bruno Hardy, \textit{Application dans l’espace de la directive 95/46/CE: la géographie du droit à l’oubli}, 2014 RTDEur. 879 (2014), at part IV; Jones, \textit{supra}, at 175-177; Julia Powles, \textit{Results May Vary: Border disputed on the frontlines of the “right to be forgotten”}, Slate (Feb. 25, 2015), http://www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html; Dan Jerker B. Svantesson, \textit{The Google Spain case: part of a harmful trend of jurisdictional overreach}, European University Institute Working Papers, RSCAS 2015/45, July 2015 (proposing a model resting on blocking results on a regional scale); Brendan van Alsenoy & Marieke Koekkoek, \textit{The extra-territorial reach of the EU’s “right to be forgotten”}, ICRI Working Paper Series, 20/2015, Jan. 19, 2015, at 14-29.

\textsuperscript{13} Duck Duck Go is a search engine launched in 2008 that brands itself as a data privacy friendly alternative to Google. Following the reveal of the NSA’s PRISM surveillance program, which heightened demand for transparent data practices, Duck Duck Go’s popularity has heightened, and it serves approximately 12,500,000 search queries per day. The company behind the search engine is headquartered in Paoli, Pennsylvania, but members of its development team are scattered all over the world, including European countries such as England, France, and Italy. \textit{See Direct queries per day}, Duck Duck Go (last visited May 10, 2016), https://duckduckgo.com/traffic.html; and \textit{About Duck Duck Go}, Duck Duck Go, (last visited May 10, 2016), https://duckduckgo.com/about. For more background information on the company, see John Paul Titlow, \textit{Inside DuckDuckGo, Google’s Tiniest, Fiercest Competitor}, FastCompany (Feb. 20, 2014), http://www.fastcompany.com/3026698/inside-duckduckgo-google's-tiniest-fiercest-competitor.
subjective right of privacy, the identification of its territorial reach is overly convoluted, inconsistent, and, as such, presents severe risks of legal uncertainty. In light of this conclusion, the paper will formulate several proposals, both de lege lata and de lege ferenda, which would cure these deficiencies. It will then conclude with some thoughts on whether or not the enactment of the GDPR will solve these issues.

Before proceeding towards the analysis proper, however, some background information needs to be provided. After a short description of the system instituted by the Data Protection Directive, the paper will summarize the Google Spain decision, and describe its fallout, including its current implementation model. Then, a deeper run-through the issues raised by the geographical scope of the RTBD will be conducted, before moving on to the case resolution exercise.

THE DATA PROTECTION DIRECTIVE

The legal framework surrounding the RTBD is Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, which was adopted by the European Union in 1995 in order to provide a comprehensive system for personal data protection across its territory and harmonize data processing practices. The Directive sets out certain key principles, such as fairness, transparency, and proportionality, which must be respected by ‘data controllers’, i.e. entities dealing with personal data and falling under the Directive’s scope of application. Through the application of these principles, the fundamental rights of the physical persons whose personal data is being used (or ‘processed’ in the language of the Directive) are safeguarded.

Due to its nature as a directive, the document does not entail the creation of a single, harmonized data protection regime all across the European Union. Rather, it provides a framework of underlying principles that needs to be transposed into the national data protection law of each Member State in order to be effective. The legal landscape of data protection in Europe is thus today still formally composed of multiple parallel national laws, each being overseen, applied, and enforced by a national organism known as a ‘data protection authority’, or ‘DPA’.

Guidance as to how the Directive should be interpreted is provided by an independent advisory board dubbed the ‘Article 29 Data Protection Working Party’, which is composed of representatives of the...
European Commission, the European Data Protection Supervisor, and each of the Member States’ DPAs. Its main task is to promote the consistent and uniform interpretation of the Directive across all Member States through the adoption of opinions and recommendations, each of these being ordinarily devoted to a specific aspect of data protection law. Because the provisions of the Directive were drafted before the advent of the commercial Internet, for the past fifteen years a substantial part of the work of the Art. 29 WP has been dedicated to their adaptation, one might even say translation, to the digital landscape. Directly relevant to the topic of this paper, a few of the WP’s documents have dealt with the interpretation of the Directive’s geographical scope rules when applied to search engines and websites more generally. One can mention the Working Document on Processing of Personal Data on the Internet, the Working Document on privacy on the Internet, the Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, Opinion 1/2008 on data protection issues related to search engines, and Opinion 8/2010 on applicable law. The Art. 29 WP has also addressed the issue of the RTBD through a dedicated set of guidelines published in November 2014 – though it did not address the extraterritorial reach of the right there. And as will be shown in the next section, the Google Spain decision, i.e. the leading case in which the RTBD was first identified under the Directive by the ECJ, did not provide much guidance on that front either.

THE ECJ’S GOOGLE SPAIN DECISION

In 1998, Mario Costeja González, a Spanish resident, found himself in financial trouble and was forced to sell off real estate assets in a public auction to settle social security debts. As mandated by the applicable Spanish rules of procedure, a notice of the auction, mentioning González by name, was published in the local newspaper La Vanguardia in order to attract bidders. The notice, along with the rest of that day’s edition,
was then scanned and added to the archives of the newspaper’s online website. 28 Around ten years later, González, now in a better financial situation, performed a Google search using his own name and discovered that one of the top results served by the search engine was the notice published in the La Vanguardia. Arguing that having this, now irrelevant, notice published so prominently in relation to his name was harming his reputation, M. Gonzales asked both La Vanguardia and Google Spain, a subsidiary of the California-based search engine located in Madrid, to remove the original notice and the search link leading to it. Both of these entities refused.

González then filed a complaint requesting the same two removals in front of the Spanish DPA, the Agencia Española de Proteccion de Datos. 29 On July 30, 2010, the latter issued a decision rejecting the request with regards to the notice present in the archives of the La Vanguardia’s website; being mandated by law, this publication was protected. At the same time, finding that Google Spain and Google Inc. were not protected by a similar exception, it ordered them to take down the search results pointing towards the notice. 30 To say the least, Google was not pleased with this result, and it appealed the decision in front of the National High Court of Spain, the Audiencia National.

Formally, the law applicable to the case was the Spanish data protection law, the Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal. Google’s appeal, however, focused on the greater principles contained in the Data Protection Directive. In particular, the company argued that its activity as a search engine fell outside of the Directive’s personal and material scope and that any request for removal had instead to be addressed to the original publisher, in this case the La Vanguardia newspaper. In addition, it contended that, being a US based corporation performing data processing operations there, the Directive could not apply, geographically speaking, to its activity. Finally, it asserted that, while the principles of the Directive grant a general right to erasure of unlawfully processed personal data, they do not imply the right to request the removal of search results linking to harmful, embarrassing, and outdated, but lawful, protected, and available, material. Because these questions concerned unsettled questions regarding the interpretation of the Directive, the Audiencia National referred them to the European Court of Justice for further clarification.

On June 25, 2013, Advocate General Jääskinen published his opinion, 31 which generally agreed with Google and emphasized that search engines, which do nothing more than provide access to content published by third parties, 32 should not be burdened with the task of implementing such an extended right to erasure. 33 He also underlined the risk that such a right would pose to the right to information, and correspondingly also expressed concerns about censorship. 34 None of these considerations survived in the final judgment rendered by the ECJ on May 13, 2014, which, broadly summarized, established that search engines were

29 Hereafter referred to as the ‘AEPD’.
30 Summarized in Audiencia Nacional, Sala de lo Contencioso, Google Spain c. Agencia de Proteccion de Datos, N° de Recurso: 725/2010. See also Google Spain, Case C-131/12, at pars. 14-17.
32 Id., at pars. 86-90.
33 Id., at par. 108.
34 Id., at par. 133.
included in the scope of the Directive, that the fundamental rights to privacy granted to data subjects applied to search results independently of how they applied to the original content they link to, and that, consequently, Google, along with every other search engine, was bound to comply with individual requests – such as the one filed by González – asking for the removal of links, displayed following a name search, leading to “inadequate, irrelevant or no longer relevant” personal information. In other words, the Directive granted to data subjects a ‘Right to be Delisted’, which could be directly exercised against search engines.35

Regarding the issue of the right’s geographical implications – and without entering too much into the specifics of the decision, as an in-depth analysis of its reasoning will be provided in the later sections of this paper – the ECJ found that, since Google had its Google Spain subsidiary located in Madrid, the conditions of article 4 (1) (a) of the Directive, which foresees the application of national data protection law when the establishment of a data controller is located in a Member State, were fulfilled, meaning that it was subject to the principles of European data protection law including the RTBD.36 The Court did not, however, go in any way beyond this conclusion. Google Spain, thus, does not say anything about the possible application of EU law to foreign Internet intermediaries having a lesser presence in Europe than Google, nor does it provide a framework for the geographical scope of the RTBD going beyond the basic scope rules of the Directive.

Scholarly reactions to this specific point in the decision have been polarized. Some critics perceived Google Spain as an unprincipled, unilateral extension of European law. Left unchecked, the decision bears the risk of submitting all search engine operators – regardless of the location of their headquarters and of the place of their business activities – to the RTBD, thus elevating European concepts of personal privacy as the de facto law of the land of the Internet.37 In turn, this raised concerns about lack of comity with other laws which, like US data protection law, include no such obligations.38 Responding to these views, other commentators pointed out that the finding that Google was bound to apply the RTBD was not by itself an unprincipled extension of European data protection law, given the company’s role as the primary search engine for users located in the European Union and the fact that it held many assets in several Member States. On the contrary, reaching the opposite conclusion would have created an unwanted gap in the scope of the Directive, allowing search engines that knowingly bring their business to the European Union to escape their obligations regarding the search results they publish about European citizens.39 Viewed in this light, Google Spain stood not for the universal application of European data protection law, but for the more

35 Google Spain, Case C-131/12, at pars. 35, 81-88.
36 Id., at pars. 45-60. For an in-depth analysis of this part of the decision, see infra, at 29-32.
38 Jones, supra, at p. 55-80; Rustad & Kulevska, supra, at 379-380 (showing that there is no all-encompassing right to privacy in the US, which directly clashes against the RTBD).
39 Peers, supra, (“[I]t would be remarkable if Google, having established a subsidiary and domain name in Spain and sought to sell advertising there, would not be regarded as being ‘established’ in that country.”); Svantesson, supra, at 6-7; van Alsenoy & Koekkoek, supra, at 13. Highlighting that the RTBD, as a right existing between national and regional conceptions of free speech and data privacy, is a “matter of boundary disputes, informed by culture and history”, see Julia Powles, Swamplands of the Internet: Speech and Privacy, Ion Magazine (Feb. 11, 2015), http://www.ionmag.asia/2015/02/swamplands-internet-speech-privacy/.
reasonable proposition that foreign Internet-based businesses that transact with persons located on EU territory are subject to local regulation.

Many authors, however, agreed that the ECJ failed to provide sufficient details regarding the extraterritorial boundaries of the RTBD in its decision. Notably, the question of whether it applied to foreign non-Google search engines – and of what standards should be used to determine this issue – was left open. In addition to the general uncertainty about the extraterritorial reach of the RTBD, the chosen implementation model of that right, towards which this paper will now turn, raised an additional set of issue geographical scope issues – this time of a more internal character.

**CURRENT IMPLEMENTATION MODEL**

A few days after the publication of the *Google Spain* decision, Google moved to implement it by setting up, on May 30, 2014, a dedicated form allowing its European users to request the removal of search results. To do so, any given claimant must provide her full name, choose a European country of affiliation – a selection which will determine the geographical *locus* of the claim – and attach a valid digital form of identification. Then, she may state which search results she wishes to see removed, and for what reason. Each claim is adjudicated by an internal procedure set up by Google specifically for this end, leading either to the removal of the link or links, or to the rejection of the request. In order to adequately decide in each case, the company, through the work of a specially-appointed independent Advisory Council, drafted a set of guidelines detailing some criteria under which each RTBD claim is examined. Examples of these criteria include the claimant’s role in public life, the nature (whether public or private) of the information contained on the web page linked to by the search result, and whether this information is fresh or outdated. Google’s guidelines, for the most part, follow those published by the RTBD claim.

---

40 Kuner, supra, from the same author, see also *The right to be forgotten and the global reach of EU data protection law*, Concurring Opinions (June 1, 2014), http://concurringopinions.com/archives/2014/06/the-right-to-be-forgotten-and-the-global-reach-of-eu-data-protection-law.html; Rustad & Kulevska, supra, at 366; Spiros Tassis & Margarita Peristeraki, *The Extraterritorial Scope of the “Right to Be Forgotten” and how this Affects Obligations of Search Engine Operators Located Outside of the EU*, 3 E.N.L.R. 244, 250 (2014); Jonathan Zittrain, *Is the EU compelling Google to become about.me? The Future of the Internet and How to Stop it* (May 13, 2014), http://blogs.harvard.edu/futureoftheinternet/2014/05/13/is-the-eu-compelling-google-to-become-about-me/.

41 *Search removal request under data protection law in Europe*, Google (last visited May 9, 2016), https://support.google.com/legal/contact/lr_eudpap?product=websearch#.

42 As will be discussed further in this contribution, this practice does not align with the way in which the Directive determines the scope of application of local data protection law, see infra, at 40.

43 The Advisory Council, which was established by the company around August 2014, took part in several meetings conducted in major European cities. The Council was composed of various scholars, policy makers and stakeholders such as *Le Monde*’s editorial director Sylvie Kaufmann, human rights analyst Frank La Rue, former Spanish DPA director José-Luis Piñar, and Wikimedia’s founder Jimmy Wales. More information on the group, including access to archives of their meetings and to their report, can be found at *Google Advisory Council*, Google (last visited May 10, 2016), https://www.google.com/advisorycouncil/. For a critical view of their efforts, see Eerke Boiten, *Google’s lip service to privacy cannot conceal that its profits rely on your data*, The Conversation (Feb. 16, 2015), http://theconversation.com/googles-lip-service-to-privacy-cannot-conceal-that-its-profits-rely-on-your-data-37592.


company, beyond providing some basic statistics, has kept mostly to itself and in particular has not published any of its individual decisions.\textsuperscript{46}

Aside from Google, other search engines have implemented a similar search removal form. This is the case of Microsoft’s Bing\textsuperscript{47} and Yahoo.\textsuperscript{48} The landscape of the RTBD is thus rather fragmented, since, in order to scrub results in an efficient matter, a person must simultaneously file the same request with all major search operators, without the guarantee that all of them will agree to the same result.\textsuperscript{49} In addition, gaps exist due to the fact that some search engines, such as Duck Duck Go\textsuperscript{50} or Lycos\textsuperscript{51} have not implemented the RTBD at all. In practice, though, these issues are overshadowed by Google and its dominance in the search market, as most of the deletion requests are solely targeted towards it and not towards any of its competitors.\textsuperscript{52}

With search engines assuming the role of both decision-maker and enforcing authority, DPAs have only played a secondary role, serving as appeal organisms in cases in which a search engine has denied a search result removal request. A recent investigation has shown that less than 2\% of all rejected requests are pursued in front of a DPA, hinting at the fact that data subjects are usually content with the search engine having the last word. The report also indicates that DPA practices concerning RTBD complaints are not uniform due to the fact that each of these authorities is regulated by its own national data protection law, its own set of procedural rules, and its own standards when it comes to personal privacy.\textsuperscript{53} Google’s own experiences with

\textsuperscript{46} Julia Powles, \textit{The Case}, supra, at 599-602. In response to Google’s lack of transparency, a group of 80 academics penned an open letter requesting that the company release more information on its decision making process. While it did make some more statistics available shortly afterwards, it has not responded to their call for a more open adjudicatory process. See Ellen P. Goodman et al., \textit{Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data}, Medium (May 14, 2015), http://bit.ly/1TzGSl5.

\textsuperscript{47} Request to Block Bing Search Results in Europe. Bing (last visited May 10, 2016), https://www.bing.com/webmaster/tools/eu-privacy-request.


\textsuperscript{49} This situation gave rise to services, such as the Forget.me website, allowing claimants to query multiple search engines by filing a single RTBD request. See Frequently Asked Questions, Forget.me, (last visited May 9, 2016), https://forget.me/faq. This quandary has not escaped the European legislator, either, as article 17, par. 2 of the GDPR contains a rule mandating recipients of RTBF requests to “take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data”.

\textsuperscript{50} Duck Duck Go, supra.


\textsuperscript{52} Patrick Teffer, \textit{Europeans give Google final say on ‘right to be forgotten’}, Euobserver (Oct. 8, 2015), https://euobserver.com/investigations/130590. On the role of Google as the central decision-maker regarding the RTBD, contrast Eldar Haber, Privatization of the Judiciary, 40 Seattle U. L. Rev. (forthcoming September 2016); Edward Lee, \textit{Judge Google: Why the EU Should Embrace Google’s Role in the Right to be Forgotten}, Huffington Post (May 07, 2015) http://www.huffingtonpost.com/edward-lee/judge-google-why-the-eu-s-b_7232688.html and Abril & Lipton, supra, at 380-386; Martial-Braz, supra, at par. 8 (criticizing the privatization of the decision-making process regarding the RTBD); Julia Powles, \textit{The Case}, supra, at 593-604 and, from the same author and specifically on this issue, Julia Powles & Enrique Chaparro, \textit{How Google determined our right to be forgotten}, The Guardian (Feb. 18 2015 02:30 EST), http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search.

\textsuperscript{53} Teffer, supra. Also noting the risk of trans-jurisdictional incoherence of the RTBD, see Abril & Lipton, supra, at 384-385; Ahmed, supra, at 183; Jones, supra, at 165-166 (stating that “legal interoperability” remains a major challenge); Powles, \textit{The Case}, supra, at 611 (noting that “European data protection, at present, is a bureaucratic, cumbersome, inefficient, largely unharmonized system” with each DPA having its own “ideas, cultures, and practices” and that the Art. 29 WP guidelines, while helpful, “demonstrated an unwillingness to provide detailed oversight and rigorous examination of actual cases, in favor of positional statements and ‘trust us’ assertions.”). From a broader perspective, legal fragmentation is indeed one of the biggest challenges facing search engines and Internet intermediaries: on that aspect, see Aleksandra Kuczerawy & Jef Ausloos, NoC Online Intermediaries Case Study Series: European Union and Google Spain, in Urs & Wolfgang Schulz, Governance of Online Intermediaries, Observations From a Series of
DPAs correlate these findings, as it has observed that each of them handles the specifics of the RTBD quite differently.\textsuperscript{54}

In summary, beyond the general directions provided by the ECJ in \textit{Google Spain}, the RTBD as currently implemented is, in two respects, subject to a risk of fragmentation: first, due to the plurality of search engines bearing the task of directly implementing it, though Google’s current preeminence in that market does well to hide this risk; second, due to the fact that, also at the DPA level, there are no commonly agreed-upon standards of RTBD claim management, though the current focus on Google as the main gatekeeper of the RTBD along with the lack of appeals to local DPAs, again, tends to overshadow the issue. This fragmentation is not in and of itself surprising, as the Directive does not formally harmonize European data protection laws, and as issues of personality, privacy, and free speech rights – substantive elements that come into play when deciding upon each individual removal request – have yet to be harmonized in any way across the European Union.\textsuperscript{55} The identification of such a problem, however, does raise the question of how DPA jurisdiction is, or should be, distributed across the different Member States with regards to each individual RTBD claim, and of which national laws should apply.

**DEFINING THE GEOGRAPHICAL SCOPE OF THE RIGHT TO BE DELISTED**

Taking the point of view of a search engine headquartered outside of the EU, this paper will seek to elucidate two questions. The first one is the question around the sort of links with Member States of the European Union that are considered strong enough to warrant a particular search engine being subject to the RTBD. This question boils down to a general appreciation of the extraterritorial limits of the right. The second question is more specific in nature: if the foreign search engine has not implemented the RTBD or if it refuses to do so as a matter of policy, then it may be asked which Member State DPA or DPAs would have jurisdiction for individual persons to file RTBD claims against it, and which national law would apply to each of these claims. Also included in this second question is an appreciation of whether or not the personality of each claimant – the geography of her contacts with the European Union, or the lack thereof

\textsuperscript{54} Private conversation with Peter Fleischer, member of Google’s Global Privacy Counsel, conducted at the Berkman Center for Internet & Society (Dec. 4, 2014). It was discussed that there are “multiple Rights to be Forgotten” across the European territory, rather than a single, uniform notion

\textsuperscript{55} The law of defamation and privacy torts in general is still, to this day, one of the most controversial objects of European law. In 2007, during the negotiations leading to the enactment of the Rome II Regulation, the lack of a consensus among Member States and stakeholders on the equilibrium between privacy and personality rights against freedom of speech led to the exclusion of these torts from the Regulation’s harmonization of conflict of law rules, as stated in its article 1 (2) (g). A further report mandated by the European Commission underlined that there was little hope of formulating a conflict of law rule that would pass over this political impasse, let alone trying to harmonize the various privacy regimes found across the European Member States. See Mainstrat, \textit{Comparative Study on the Situation in the 27 Member States as Regards the Law Applicable to Non-Contractual Obligations Arising Out of Violations of Privacy and Rights Relating to Personality}, JLS/2007/C4/028 Final Report, February 2009. Since then, efforts in this direction have not progressed any further; see Procedure file, Amendment of Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II), 2009/2170(INL), European Parliament Legislative Observatory (last visited on May 10 2016), \url{http://www.europarl.europa.eu/oeil/} (search for “864/2007”). For further references along with a detailed presentation of the events leading to a fractured privacy landscape in the European Union, see Michel Reymond, \textit{La compétence internationale en cas d’atteinte à la personnalité par Internet} 207-231 (2015). Arriving at the same conclusion in the context of the RTBD, see Jones, \textit{supra}, at p. 30-46 (“Each European country has a different history when it comes to data, speech, access, public interest, public figures, privacy, identity, reputation, self-determination, and self-presentation.”).
– impacts this determination in any meaningful way. As a whole, the following exercise will not only determine whether or not smaller search engines located outside of the EU, such as Duck Duck Go, must implement the RTBD; it will also test whether or not the geographical scope of the right may be ascertained in a clear and foreseeable way in situations that do not involve Google, or if its rules break down as soon as one leaves this actor-specific mindset.

As mentioned above, guidance on these matters is sparse: neither the ECJ nor the Art. 29 WP have provided clear ad-hoc rules regarding the spatial application of the RTBD. The present analysis will thus be based on the basic geographical scope rules of European Data Protection as found in the Data Protection Directive; it will observe how they operate and react when applied to situations involving specific RTBD claims. This will be performed through the resolution of a series of hypothetical cases inspired by real-life situations. These are as follows:

- **Case 1**: A1, a Spanish citizen, living in Madrid, wishes to remove a link present on search engine B1. B1’s main offices are located in Mountain View, California, and the company owns subsidiaries in Spain, Ireland, and France. These subsidiaries are not involved in the serving of search results, and instead manage local business affairs, such as the selling of advertising space.

- **Case 2**: A1, a Spanish citizen, living in Madrid, wishes to remove a link present on search engine B2. B2’s main offices are located in Mountain View, California, and the company owns a subsidiary in Ireland.

- **Case 3**: A1, a Spanish citizen, living in Madrid, wishes to remove a link present on search engine B3. B3’s main offices are located in Mountain View, California, and the company has no presence in the European Union besides serving search results. However, two of its developers reside in France and work from there via teleconferencing.

- **Case 4**: A1, a Spanish citizen, living in Madrid, wishes to remove a link present on search engine B4. B4’s main offices are located in Mountain View, California, and the company has no presence at all in the European Union besides serving search results.

- **Case 5**: A1, a Spanish citizen, living in Madrid, wishes to remove a link present on search engine B5. B5’s main offices are located in Mountain View, California. Because of its reliance on geolocation technologies, the website is not accessible from outside of the United States.

- **Case 6**: A2, a Spanish citizen, domiciled in Scottsdale, Arizona, where she spends her days in retirement with no prospect of going back to her home country, wishes to remove links present on search engine B1.

Cases 1 through 5 are designed to test the RTBD’s geographical scope against a range of search engine providers, each one entertaining fewer and fewer contacts with the European Union. Their resolution will

---

56 It is acknowledged that the nature of this exercise is steeped in private international law methodology. However, it is submitted that a private international law perspective on the scope rules of European legislation can provide a helpful insight into their operation – and of their effect on all interested parties. In this sense, see Stéphanie Francq, L’appropriabilité du droit communautaire dérivé au regard des méthodes du droit international privé (2005).

57 Case 1 is inspired by the facts of the case in Google Spain.

58 Case 2 is inspired by the situation of the Duck Duck Go search engine, see infra, at note 13.
allow for a better understanding of where exactly the threshold lies when it comes to describing the outer limits of the right. Case 6, on the flip side, raises the issue of whether or not a person having her center of activities outside of the territory of the European Union may still make use of the RTBD against these search engines and, if so, in what capacity.

Before proceeding, two caveats must be raised regarding the scope of the present analysis. First, no account shall be taken of variations that may exist in the provisions transposing the scope rules of the Directive into national legislations. There are, admittedly, some differences in the way each Member State has devised both the jurisdictional powers of its DPA and the reach of its national data protection law; however these have been considered as unwanted deviations from the mandated rules of the Directive and, as thus, will not be explored in the present contribution.\(^{59}\) Also excluded from the following analysis is the question of the jurisdiction of national courts in relation to the RTBD, since such an exercise would, in a similar fashion, go outside of the four corners of the Directive.

JURISDICTION

All of the hypothetical cases share a common set of facts: a Spanish citizen requests a US based search engine to take down a search result, which she feels is harmful to her privacy rights. When the search engine refuses to accede to her request, she decides to bring it forward before the data protection authority of a Member State, with a preference for the AEPD, which is located in her Spanish home state. The following section will consider whether the latter has jurisdiction over the foreign search engine, and what grounds support this result; it will also consider whether DPAs located in Member States other than Spain may also receive the claim. Then, the focus of the analysis will shift from the search engine to the claimant, and will raise the question of whether her existing links with the European Union – or lack thereof – might influence this determination.

DPA JURISDICTION OVER A FOREIGN SEARCH ENGINE

Article 28 (4) of the Data Protection Directive

Both Google Spain and the Art. 29 WP guidelines envisage that, in the case that a search engine were to refuse a delisting of results, a data subject may turn towards a DPA to appeal the decision following the formal claim procedure established by article 28 (4) of the Data Protection Directive.\(^{60}\) This provision is set out in the following terms:

---

\(^{59}\) For more information on the differences between the basic scope rules of the Directive and the rules contained in national implementation law, see Lokke Morel, \textit{Back to basics: when does EU data protection law apply?}, 1 International Data Privacy Law 92, 100-101 (2011).

\(^{60}\) See Google Spain, Case C-131/12, at par. 78, and the Art. 29 WP guidelines, at 24 (“Despite the novel elements of the CJEU judgment, deciding whether a particular search result should be de-listed involves – in essence - a routine assessment of whether the processing of personal data done by the search engine complies with the data protection principles. Therefore the Working Party considers that complaints submitted by data subjects to DPAs in respect of refusals or partial refusals by search engines are to be treated – as far as possible - as formal claims as envisaged by Article 28(4) of the Directive”).
“Each supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data.”

The outer limits of the power conferred by this article to DPAs regarding the exercise of the RTBD have not been explored any further in official materials; however some general guidance may be found in the ECJ’s 2015 Weltimmo decision.61

The case concerned a series of complaints lodged before the Hungarian DPA, the Nemzeti Adatvédelmi és Információszabadság Hatóság, made against a company registered in Slovakia that operated a real estate property dealing website concerning assets located in Hungary. The complaints, which were filed by some of the website’s advertisers, arose because the company did not honor their requests of removing their advertisements past the one month trial period. Instead, it charged them for its services and eventually sent their personal details to local debt collection agencies.62 Most of the questions referred to the ECJ by the Kúria, the Supreme Court of Hungary that came across the case on appeal, concerned issues of applicable national data protection law – turning mainly on whether the Slovakian company’s presence in Hungary was sufficient in order to trigger the application of Hungarian data protection law.63 One of the questions, however, centered on the range of powers conferred to the Hungarian DPA by article 28 (4) of the Directive. If the ECJ were to conclude that Slovakian, and not Hungarian, data protection law applied to the case, what would this mean in regards to the authority of the Hungarian DPA? Would it still be able to hear out the requests? If this question were to be answered in the positive, would the DPA also be able to impose fines to the defendant, even if the applicable data protection law was not its own?

The Court answered in two steps. First, it explained that a DPA’s capacity to hear claims as granted by article 28 (4) of the Directive had to be read in conjunction with the rest of article 28 and namely its paragraphs (1), (3) and (6). Paragraph (1) stands for the general proposition that a DPA is “responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to [the] Directive”; paragraph (3) then provides DPAs with the rights of investigation and intervention they need to fulfill that mandate; finally, paragraph (6) underlines the territorial nature of these powers by stating that “[e]ach supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it.” Thusly, a DPAs attribution to hear claims under paragraph (4) of article 28, being subject to the same principles and limitations, does not hinge upon what law applies, but instead upon the presence of the complained-upon act of data processing on the territory of that DPA’s home Member State.64 In other words, a DPA may act upon claims regarding any and all acts of data processing that have taken place on their territory, regardless of which data protection law actually applies to that act.

The Court justified this solution by referring to the need of providing a forum to data subjects whose rights may be infringed by the activity of a data controller located abroad and which would otherwise be subjected

61 European Court of Justice, Weltimmo s.r.o v Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-230/14, Oct. 1, 2015.
62 Id., at par. 9.
63 Id., at pars 19-42.
64 Id., at pars. 51-52.
to the data protection law of another Member State or even a foreign country. The facts of the case at hand, which saw a Slovakian company direct its business towards Hungary while structuring its activity in order to precisely avoid the application of Hungarian law, certainly helped the Court in reaching that conclusion.\textsuperscript{65}

In a second step, however, the ECJ introduced a limiting factor. Referring to “the requirements derived from the territorial sovereignty of the Member State concerned, the principle of legality and the concept of the rule of law that the exercise of the power to impose penalties cannot take place, as a matter of principle, outside the legal limits within which an administrative authority is authorised to act subject to the law of its own Member State,” it held that a DPA, when handling a request under a law that is not its own, does not have the power to impose penalties upon the data controller targeted by the complaint. In those cases, the Court continued, the DPA should “in fulfilment of the duty of cooperation laid down in article 28 (6) of [the] Directive, request the supervisory authority of that other Member State to establish an infringement of that law and to impose penalties if that law permits, based, where necessary, on the information which the authority of the first Member State has transmitted to the authority of that other Member State.” Thus, even if the Hungarian DPA had jurisdiction over Weltimmo, “if the applicable law is that of a Member State other than Hungary, the Hungarian data protection authority [would] not be able to exercise the powers to impose penalties which Hungarian law has conferred on it,” meaning that its effective powers were constrained by the law applied to the case at hand.\textsuperscript{66}

In summary, the ECJ in \textit{Weltimmo} established two ground rules for determining the jurisdiction of a DPA according to article 28 (4) of the Data Protection Directive. First, each DPA has the power to act upon any request concerning an act of data processing that has taken place within the borders of its Member State; no element beyond the presence of that act in that jurisdiction is needed. Second, only DPAs that may apply their local data protection law according to the law-selecting rules of the Directive have full jurisdiction; in particular, only these DPAs are allowed to impose fines upon the data controller subject of the complaint. A DPA that only has a limited jurisdictional scope according to this second rule should consider transferring the case to one of its more suitable counterparts. Two questions thus underlie the jurisdictional analysis: where does data processing take place? And what is the law applicable to that data processing?\textsuperscript{67}

The second of these questions – which provides a certain degree of identity between jurisdiction and applicable law – will be dealt with in the choice of law portion of this paper.\textsuperscript{67} The first, which will occupy

\textsuperscript{65} \textit{Id.}, at par. 53: “In the absence of [art. 28 (4)], where the controller of personal data is subject to the law of a Member State, but infringes the right to the protection of the privacy of natural persons in another Member State, in particular by directing his activity at that other Member State without, however, being established there within the meaning of that directive, it would be difficult, or even impossible, for those persons to enforce their right to that protection.”. As the determination of which data protection law applied to the Slovakian company hinged on whether or not it had an establishment in Hungary according to article 4 (1) (a) of the Directive, its owners were careful not to create such a presence in that State. For more detail on the choice of law issue, see \textit{infra}, at 26-28.

\textsuperscript{66} \textit{Id.}, par. 59.

\textsuperscript{67} \textit{Infra}, at 25 \textit{et seq}. This implies that DPA jurisdiction hinges greatly – yet not entirely – on the question of what national data protection law applies to the proceedings at hand. On this point, \textit{Weltimmo} follows the earlier work of the Art. 29 WP; see its \textit{Opinion on applicable law}, \textit{infra}, at 10 (“Although in most cases these two concepts – applicable law and competence of supervisory authorities – tend to coincide, usually resulting in Member State A’s law being applied by Member State A’s authorities, the Directive explicitly foresees the possibility of different arrangements. Article 28(6) implies that the national data protection authorities should be able to exercise their powers when the data protection law of another Member State applies to the processing of personal data carried out within their jurisdiction.”).
the remainder of the present section, raises several issues when applied to the RTBD: what is the act of data processing relevant to the purposes of the RTBD? And where is that act located? Answering these questions entails a short side discussion of the personal and material scope of the RTBD, under the framing of how an act of ‘data processing’ is defined under the Directive.

Definition of data processing
‘Data processing’ or ‘processing of personal data’ is defined by the Data Protection Directive as “any operation or set of operations which is performed upon personal data, whether or not by automatic means,” including “collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”68 Personal data is understood as “any information relating to an identified or identifiable natural person.”69 In the context of online dealings, this term does not only include personal identifiers such as the person’s name, age or gender, but also technical identifiers, such as that person’s IP address, website activity, or search history.70 Taken all together, these definitions mean that the handling of any personal or user data will be considered as an act of ‘data processing’ under the Directive. In particular, no distinction is made regarding the source or nature of the personal data used; the ECJ held, in the 2008 Satamedia case, that the republication of public domain data extracts identifying the income of Finland’s most wealthy persons fell squarely under the definition.71

Not all acts of data processing, however, are subject to the principles contained in the Directive. As art. 3, par. 1 states, its scope of application is limited to those acts that are performed “wholly or partly by automatic means” or that “form part of a filing system or are intended to form part of a filing system.” The first condition has been interpreted as consistently applying to any data processing operation conducted on the Internet. A good example of this is the Lindqvist case, which was rendered by the ECJ on November 2003. The facts concerned a woman who was working as a catechist in a Swedish parish. Using her personal computer in her spare time, she uploaded to the World Wide Web a “mildly humorous” website containing information on herself and on 18 of her colleagues, mentioning their names and occupations. The piece attracted the attention of the Swedish DPA, the Datainspektionen, which purported to fine her for failing to properly register and announce her data processing activities. The question before the ECJ was thus whether or not the mere act of uploading personal information on the Internet was an act of ‘data processing’ performed through ‘automatic means’ as set out in art. 3 par. 1 of the Directive, thus falling under its scope of application. The court answered in the affirmative, holding that “placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the Internet,” and that “[s]uch operations are performed, at least in part, automatically.”72

69 Id., at art. 2, let. a).
70 Art. 29 WP, Privacy on the Internet, supra, at 14-17 and 21; Opinion on data protection issues related to search engines, supra, at 8-9.
71 European Court of Justice, Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Case C-73/07, European Court Reports 2008 I-09831, Dec. 16, 2008, at pars. 35-36.
72 European Court of Justice, 11.06.01, Lindqvist, Case C-101/01, European Court Reports 2003 I-12971, Jun. 11, 2001, at par. 26.
The technical and automated nature of the Internet as a communications medium thus, by itself, fulfills the criterion. The same attitude can be found in the work of the Art. 29 WP, which has held, since 1999 and in rather broad terms, that the Directive generally applies to all acts of data processing conducted over the Internet in order to ensure “trust and confidence of users in the functioning of the Internet and the services provided over it.”

Finally, the Directive defines the main person responsible for a given act of data processing falling under its ambit as a ‘data controller,’ which it defines as “the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.”

**Data processing operations targeted by the Right to be Delisted**

Search engines routinely perform many activities that may be characterized as ‘data processing’ under the Directive; however, identifying which of these activities are specifically targeted for the purposes of the RTBD requires a distinction between two separate facets of a search engine’s business model.

The first facet regards the services that are offered by the search engine directly to the end user; this includes the core search functionality but also related tools and services such as search personalization, user accounts, and other value-added propositions. In this context, the processing of personal data stems from the collection and use by the search engine of information related to each of its individual users. It may take several forms, such as the logging of their IP addresses and timestamps, the placing of cookies on their browsers, the collection of their search terms and browsing history, or the direct input of their personal details, such as when such information is required to access a personalized service. Illustrating well the means and purposes of this facet of a search engine’s data processing activities is the difference in policy between Google and Duck Duck Go. The latter uses the fact that it collects less personal user data than the former as one of its selling points; yet, because of this, it lacks some of the more convenient features of its competitor, such as access to a list of past searches and the option to have a consistent personalized search experience.

These interactions with the personal data of end users on the part of search engines do not actually raise major issues when it comes to characterization under the Directive; they have, on the contrary, been consistently interpreted as data processing operations falling under its material scope since at least 2008, when the Art. 29 WP published its opinion on search engines. These interactions are, however, irrelevant when it comes to discussing the scope of the RTBD.

Indeed, the RTBD is preoccupied with a second facet of a search engine’s business model, which is its role as a service provider of search results and related content. This facet hinges on the search engine’s various

---

74 Data Protection Directive, supra, art. 2 let. (d); for more details on this and related terms, see Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of “controller” and “processor”, WP 169, 00264/10/EN, Feb. 16, 2010; Morel, supra, at 98-99.
75 Duck Duck Go does offer some personalized settings, however they are saved on their cloud on an ‘opt-in’ basis, see Settings, Duck Duck Go (last visited May 10, 2016), http://www.duckduckgo.com/settings.
76 Art. 29 WP, Opinion on data protection issues related to search engines, supra, at 9 (“A search engine provider that processes user data including IP addresses and/or persistent cookies containing a unique identifier falls within the material scope of the definition of the controller, since he effectively determines the purposes and means of the processing.”).
relationships with the third parties that supply, or are otherwise involved with, the content that is displayed to end users following a search query. These third parties come in different degrees of involvement. First amongst those are advertisers; these, along with website owners paying for sponsored results, constitute the search engine’s main revenue source. Then, there are the owners of the websites that are included by the search engine into its results. Finally, and most importantly for the present purposes, there are all of the individuals who do not interact directly with the search engine, but whose personal information may be displayed following a name search.\(^\text{77}\) This was the situation of Mario Costeja González in Google Spain; and actually one of the key points of that decision hinged on whether or not the collection and display of third party personal information through search results could be characterized as ‘data processing’ under the Directive; meaning that, if that were the case, search engines could be liable as ‘data controllers’ for this activity. Contrary to the case of end user data, this question was still unsettled in European Law at the time – and for example, the Art. 29 WP, in the aforementioned 2008 opinion on search engines, seemed to consider that search engines lacked sufficient control over the personal data they republish in order to fit the characterization, yet it did so on very uncertain terms.\(^\text{78}\)

With other scholars having commented on Google Spain from the standpoint of the material scope of the Directive,\(^\text{79}\) it will suffice for the present purposes to relate that the ECJ in Google Spain construed the RTBD as directed against the following acts of data processing:

\[
\text{[The] activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as ‘processing of personal data’ . . . when that information contains personal data and, . . . [that] the operator of the search engine must be regarded as the ‘controller’ in respect of that processing.}\(^\text{80}\)
\]

The RTBD thus targets the series of technical steps that form part of the act of serving search results to the end user. Since article 28 (4) of the Directive allocates DPA jurisdiction depending on the geographical location of processing, the next section will aim at determining where these technical steps actually occur. This requires a prior short presentation of what they entail from a technical perspective.

---

\(^{77}\) On the two facets of a search engine’s business model, Art. 29 WP, Opinion on data protection issues related to search engines, supra, at 6 (“The profitability of . . . search engines generally relies on the effectiveness of the advertising that accompanies the search results. Revenues are generated in most cases by a ‘pay per click’ method. In this model, the search engine charges the advertising company whenever a user clicks on a sponsored link. Much research into the accuracy of search results and advertisements is focused on the right contextualisation. In order for the search engine to produce the desired results and to properly target the advertisements in order to optimise revenues, search engines try to gain as much insight as possible into the characteristics and context of each individual query.”); Hardy, supra, at part I.

\(^{78}\) Art. 29 WP, Opinion on data protection issues related to search engines, supra, at 14. On one hand, the WP considered that search engines, “to the extent that [they] act purely as an intermediary, . . . should not be considered to be the principal controller with regard to the content related processing of personal data that is taking place.” Yet, it acknowledged that “[w]ith regard to the removal of personal data from their index and search results, search engines have sufficient control to consider them as controllers (either alone or jointly with others) in those cases, but the extent to which an obligation to remove or block personal data exists, may depend on the general tort law and liability regulations of the particular Member State.” It also carved out an exception for so-called ‘value added’ operations, which do fall under the scope of the Directive.

\(^{79}\) Van Alsenoy, Kuczcerawy, & Ausloos, supra, at 9-19; Peers, supra.

\(^{80}\) Google Spain, Case C-131/12, at par. 41; see also Hardy, supra, at part II.
Processing operations involved in search engine activity

There are four basic steps involved in the serving of search results; these are known as crawling, indexing, ranking, and display, with each of them corresponding to a distinct act of data processing. The first two steps, crawling and indexing, are related to how the search engine constitutes a searchable database of web pages, or ‘search index’, and they take place without the input of the end user. The remaining two steps, ranking and display, occur at the moment that a search is performed.  

Search engines do not actively search the entire World Wide Web each time a user performs a web search; instead they rely on an internal ‘search index’ – a searchable database of web pages allowing for easy keyword identification and fast retrieval. The first step in making a working search engine is about populating this index by discovering new web pages; this act is referred to as ‘crawling.’ Typically, this is performed by programs known as ‘web crawlers’ or ‘web spiders’ that have the ability to scan and parse entire web pages – including their text, titles, keywords, and any links they might contain – in a matter of seconds. Once a web crawler has finished retrieving a given webpage, it follows each link present on that page and starts its work anew. As each of these new pages might, in turn, contain other links pointing to further web pages, a large quantity of content can be discovered in a manner of seconds by these automated robots. The particular behavior of each web crawler – for example how often it performs a scan, on which websites and how deep it should go when following links – is set by the search engine operator.

The most well-known generalist search engines, such as Google, Yahoo!, and Bing, crawl the World Wide Web at large in order to index as many web pages as possible; this model is however not the only one, and for example the Swiss Search.ch search service mostly limits its crawling activity to websites under the Swiss .ch top level domain in order to retain its focus on local affairs. Finally, search engines usually follow the robots exclusion standard, which allows website owners to signal to web crawlers that they wish to exclude their site from being indexed by including of a small text file labeled “robots.txt” on their server. The standard is, however, more of a de facto agreement than a binding obligation.  

Once the web crawler has discovered and processed a given web page, it creates a copy of it, along with its address or Universal Resource Locator (‘URL’), keyword information, and other parsing data and sends it for inclusion and storage into the search index alongside every other web page already processed. This is the indexing step, which sees all of the information collected by the web crawlers aggregated into a single searchable database in a matter of seconds. In order to store and process all of that content, search engine operators make use of large data centers, whose location is usually kept undisclosed for competition purposes. These data centers

---


83 Search.ch (last visited May 10, 2016), http://www.search.ch. It also includes limited access to other domain names.


86 This fact belies one of the difficulties faced by the ECJ in *Google Spain*, as the actual processing leading to the display of the results complained about by Mario Costeja González took place in such data centers and not at the firm’s Spanish subsidiary; see the decision at par. 43 (“The information indexed by its ‘web crawlers’ or robots, that is to say, computer programmes used to locate and sweep up the content of web pages methodically and automatically, is stored temporarily on servers whose State of location is unknown, that being kept secret for reasons of competition.”). For more background information, see *Inside our data centers*, Google (last visited May 10, 2016), https://www.google.com/about/datacenters/inside/; Sam Shead, *Google is planning a
power the whole infrastructure of the search engine, and in particular house all of the elements that are made visible to the end users, i.e. the search engine website, its features, and the results it provides.

The third step, ranking, occurs each time a user performs a search and consists in the search engine using a set of criteria – altogether referred to as a ‘search algorithm’ – determining which of the pages stored in the search index are the most relevant in regards to that user’s query. For example, if user A enters the term “cat,” the search engine will not just produce a list of the websites it holds and mentioning cats; it will also rank the results by asking some further questions: which of these pages is the most visited? Are any of these pages current news stories which may be of topical importance? Are there any pages, such as the Wikipedia entry on cats, which may be considered as qualitative safe bets? Are any of these pages “fresh,” meaning updated recently? Does the search engine know what sort of content is preferred by the user? Each search engine holds its own set of ranking algorithms, as the quality of the resulting list is one of the major defining traits of any of them. Finally, once the list of results is established, it is, as a last step, served to the end user and displayed on her machine, whether a computer or a smart phone, at the place in which she is located.87

The four-step model is a good baseline for formulating how search engines work – and it helps that it accurately describes the operations performed by the most well-known of these services, such as Google, Yahoo!, and Bing. However, account must be taken of alternate methods for serving search results; two examples can be mentioned in this regard. First, search engines may allow website owners to bypass the crawling step by manually submitting their content for inclusion into the index; in the early days of the Internet, this was actually the main procedure for having one’s content referenced by a search engine.88 Second, services referred to as ‘meta search engines’ do not mainly rely on crawling or indexing; instead they function by forwarding the search query entered by a user to a series of other search engines, and then by scraping, correlating, ranking, and serving the multiple result lists they have obtained through those other services.89 Duck Duck Go rests upon this technology (though only partly),90 as does Dogpile.91

87 Grehan, supra, at 22-36.
88 Most famously, Yahoo! started out as a hand curated directory of websites before morphing into a modern search engine; see Danny Sullivan, The Yahoo Directory, Once the Internet’s Most Important Search Engine - Is To Close, Search Engine Land (Sep. 26, 2014), http://searchengineland.com/yahoo-directory-close-204370. Nowadays, some search engine still offer the opportunity for website owners to submit their content, though this typically results in the addition of that link to their crawler’s route. See Search Console, Google (last visited May 10, 2016), https://www.google.com/webmasters/tools/submit-url; Submit your Site to Bing, Bing (last visited May 10, 2016), http://www.bing.com/toolbox/submit-site-url.
89 See Different Engines, Different Results, Dogpile (April 2007), http://www.dogpile.com/support/Metasearch (follow the link for the full study), at 3 (“The goal of a metasearch engine is to mitigate the inherent differences of single source search engines thereby providing Web searchers with the best search results from the Web’s best search engines. Metasearch distills these top results down, giving users the most comprehensive set of search results available on the Web.”). The distinction is not all-encompassing, either, some results of crawling-based search engines may also be funneled by reference to a shared database or repository, see Grehan, supra, at 6-7 (mentioning the examples of the pre-Bing MSN search engine, Hotbot and Yahoo!); see also the Duck Duck Go example in the following note.
90 Source, Duck Duck Go (last visited May 10, 2016), https://duck.co/help/results/source (“In fact, DuckDuckGo gets its results from over four hundred sources. These include hundreds of vertical sources delivering niche Instant Answers, DuckDuckBot (our crawler) and crowd-sourced sites (like Wikipedia, stored in our answer indexes). We also of course have more traditional links in the search results, which we primarily source from Yahoo!, and in some regions and scenarios, Yandex and Bing.”).
Locating the place of processing
So, where does the processing occur for the purposes of article 28 (4) of the Directive? Since the supply of search results relies on a series of technical operations that, as shown above, operate in different kind of spaces, one may identify three different anchor points: the place of crawling, the place of indexing and ranking, and the place of display. In this section, a discussion of the value of these places as jurisdictional connecting factors will be performed.

Place of crawling
First is the place of crawling, which may be defined as the place in which the servers that have been visited by a search engine’s web crawler are located. Due to the decentralized way in which the Internet works, the servers hosting the content of a particular website may be located in one or several jurisdictions depending on that website’s IT policy and hosting arrangements. Furthermore, the same information might be hosted on several different servers located in different parts of the world in order to reduce latency. Identifying where exactly the crawling occurs in a geographical sense is thus, it is submitted, a challenging exercise. Furthermore, due to these same features, the place where a website has been crawled by a search engine has no real connection to the geographical dimension of that website’s activity and use of personal data. In Google Spain, for example, there was no question that the facts at hand were centered on Spain: La Vanguardia is a Spanish newspaper, the notice it published concerned a local auction, and González himself is established in that country. Yet, the act of Google crawling that web page might happen anywhere depending on the hosting practices of the newspaper’s website; its servers might be present in Spain, in other Member States, or even in non-EU countries. Should, by hypothesis, the Polish DPA have jurisdiction over Google because its web crawler happened to visit a server located there?

One may raise the argument that major search engines like Google and Yahoo!, in order to provide a wide range of relevant results, cast their metaphorical nets in the widest possible fashion; it could thus be tempting to sidestep these issues by generally stating that crawling happens everywhere at once and leave it at that. Such a position however fails to address the situation of smaller search engines that operate on a local basis. Coming back to an example mentioned earlier, the Search.ch service mostly provides links to websites making use of Swiss domain names ending in “.ch,” thus defeating the “wide net” presumption. Yet, the problem of locating the websites it crawls remains entirely whole since a website making use of a Swiss domain name does not necessarily store its content on servers located in Switzerland, and does not necessarily cater only to a Swiss audience. Another example challenging the relevance of crawling as a jurisdictional geographical connecting factor is the case of meta search engines like Duck Duck Go and Dogpile. These do not rely on crawling the World Wide Web at large and instead scrape search results served by other competing search operators. Technically speaking, then, their place of crawling — or at least of the data processing operation closest to that term — is defined by where these other search engines process their own data and bears no relation to the information served as search results.

92 See supra, at 19.
These difficulties suggest that, while crawling is, by definition, a processing operation relevant for the purposes of determining DPA jurisdiction under article 28 (4), it is a purely technical function that does not work entirely well when considered as a jurisdictional connecting factor.\(^93\)

**Place of indexing and ranking**
Less problematic than the place of crawling is the place of ranking and indexing, i.e. where the search engine stores all of its data, and where that data is parsed, organized, and ranked. It corresponds to an identifiable physical location – where the operator has established its data centers. There is thus no difficulty in characterizing this place as an anchor point for DPA jurisdiction under article 28 (4) of the Data Protection Directive. And while search engine operators usually keep tight wraps over the location of these data centers, their identification may be mandated by a DPAs power of investigation conferred by article 28 (1), first indent.

**Place of display**
The last possible connecting factor is the place of display of search results, which may be understood as designating the location of the end users' devices accessing and using the search engine. Since it correlates with the search engine's act of making its service available to the end users it serves – along with the display of sponsored results and advertisements, this connecting factor is both reasonable and easy to locate, as one will just need to identify where that search engine carries out its business.

One issue when considering its use in the context of individual RTBD claims is whether or not it should be required for the claimant to prove that the specific search result that is the target of her removal request has been displayed in the territory of her DPA of choice in order to justify the latter's jurisdiction over the foreign search engine, or if a general showing that the search engine displays its results there would be sufficient to that end. Given the protective nature of article 28 (1) regarding the rights of data subjects, it is submitted that it should not be interpreted too restrictively, and that such a requirement would go against the provision's goal of allowing data subjects to enjoy a wide access to DPAs.\(^94\) Besides, proving the publication of a single search result seems an exceedingly difficult task.

It is acknowledged that relying on the place of display of search results as a connecting factor will more often than not result in multiple DPAs having parallel authority over a single foreign search engine when that search engine chooses to display its results in more than a single Member State. However, fears about forum shopping or about seeing search engine operators being simultaneously subjected to the authority of a plethora of DPAs should not be overstated. Following Weltimmo, only DPAs whose local data protection law applies have the power of imposing fines upon the person responsible; those whose national law is not applicable to a particular request are instead bound to transfer the case to one of its more suitable

---

\(^93\) For these same reasons, the place where a server is situated has consistently been rejected as a jurisdictional connecting factor when it comes to jurisdiction over online privacy and defamation torts; see High Court of Australia, *Dow Jones v. Gutnick*, [2002] HCA 56, Dec. 10 2002, at pars. 41-44; Court of Appeal (Civil Division) (England), *Lewis v. King*, [2004] EWCA Civ 1329, Oct. 19 2004, at pars 28-31, and, implicitly, European Court of Justice, *eDate Advertising GmbH v. X*, Cases C-509/09 and C-161/10, European Court Reports 2011 I-10269, Oct. 25. 2011. For further details and references, see Reymond, *supra*, p. 233-244.

\(^94\) Furthermore, the Directive is designed to apply to data processing activities taken as a whole, see, by analogy, Art. 29 WP, *Opinion on applicable law, supra*, at 24.
counterparts. In other terms, allowing RTBD claimants to enjoy a wide range of initial DPA selection for filing a RTBD request is not problematic in and of itself because the Weltimmo rule will then concentrate the proceedings in such a way that suits the law-selecting rules of the Directive. Whether these are appropriate regarding the RTBD is another matter entirely – though one that will be covered in detail in a further section of the present paper.

With these three places of processing now identified, one can turn towards their application in the example cases.

**Application to the example cases**

In all cases except cases 5 and 6, Spanish citizen A1 will be able to file her claim against the American search engine in front of the Spanish DPA; alternatively, she may also do so in front of the DPA of any other Member State of the European Union. This is so because, by displaying search results all across the territory of the European Union, search engines B1 to B4 have triggered the authority of each respective DPA over the acts of data processing they have committed on their territory. And though it may at first blush seem unreasonable to allow A1 to pick and choose a DPA from this large selection, this problem is mitigated by the fact that only a DPA allowed to apply its national data protection law by the Directive will have full jurisdiction, including the right to impose sanctions, over the foreign search engine. This, however, does raise the question of whether the law-selecting rules of the Data Protection Directive are appropriate; the final word on these cases will thus have to wait on the resolution of this particular issue.

In case 5, the American search engine B5 does not serve search results to users located in the European Union, however, it may have, in the course of its activity, crawled websites hosted on servers located on the territory of European Member States. The ECJ’s wording in *Google Spain*, in which it considered that the act of “finding information published or placed on the internet by third parties” is a processing operation included into the scope of application the RTBD, suggests that this contact may be sufficient under article 28 (4) to confer jurisdiction to DPAs located in those Member States. Yet, that result seems unsatisfactory because search engine B5 does not bring its business in to the European Union; furthermore, any order of search results removal pronounced against it would only impact search queries performed outside of the EU. This case goes to show that the place of crawling does not seem quite fit as a jurisdictional anchor.

Finally, in case 6, DPA jurisdiction will be appraised in a similar manner as in cases 1 to 4, since the search engine’s contacts with the European Union are the same. However in this case there is a further complication due to the fact that the claimant, being domiciled in the American State of Arizona, where she spends her retirement years, has no link to Spain beyond her nationality. It might thus be argued that allowing her to file a takedown request before the Spanish DPA would constitute a form of forum shopping – as evidently she would not be able to invoke the RTBD in her home courts.

The next section will thus turn towards this remaining issue when it comes to determining jurisdiction; that is whether or not the exercise of the RTBD before the DPA of a given Member State requires some sort of

---

95 Supra, at 12-15.
96 *Infra*, at 25 *et seq.*
97 Fearing this sort of configuration, see Kuner, *The global reach of EU data protection law*, supra.
link between the claimant and that Member State, and, if that is the case, whether this requirement is effective to discourage requests emanating from persons having only a tenuous relationship with the legal order of the European Union.

**LIMITING FACTOR: THE CLAIMANT’S LINKS WITH THE EUROPEAN UNION**

**Standard**

Under article 28 (4) of the Data Protection Directive, ‘any person’ may place a request in front of a given DPA as long as the other conditions of the provision are met. There is thus no particular requirement that this person be affiliated with that Member State in any way. This rule is in line with the broader structure and goals of the Directive, which purports to offer to all physical persons—without geographical distinction— the protection of their fundamental rights against acts of data processing falling under its scope.  

Case in point, the Directive defines its geographical scope exclusively through an assessment of the relationship between the data controller and the legal order of the European Union, with no existing provision coming in to narrow down the exercise of the rights it confers to a given set of beneficiaries. The Art. 29 WP has emphasized this aspect of the Directive’s scope on multiple occasions. In its 2003 Working Document on the application of EU law to non-EU websites, it stated that “[t]he Directive makes no distinction on the basis of nationality or location because it harmonises Member States laws on fundamental rights granted to all human beings irrespective of their nationality. Thus, . . . the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen.”  

In its 2010 opinion on applicable law, it further opined that it would not be “acceptable to reduce the scope of protection [granted by the Directive] to persons residing in the EU, since the fundamental right to protection of personal data is enjoyed regardless of nationality or residence.”

The ECJ did not address the question of who should be granted the right to exercise the RTBD in the *Google Spain* decision; it seemed however to implicitly rely on the same principle of global protection. It referred, all throughout its decision, to all ‘data subjects’ in general as the beneficiaries of the right; it also mentioned with approval that article 28 (3) of the Data Protection Directive allows ‘any person’ to file a request before a DPA. Thus, it seemed at that moment that the RTBD was to be granted to everyone, regardless of residence or nationality.

---

98 *Data Protection Directive, supra*, art. 2: “In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data”.

99 See for example art. 2 (a) of the Directive, which defines that a data subject “is one [physical person] who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.” No mention is made here of any required link with the European Union. In this sense, see also Hardy, *supra*, at part III B.

100 Art. 29 WP, *Application of EU data protection law to non-EU based web sites, supra*, at 7. The Working Party, in that section, referred to application of local law to foreign data controllers according to article 4 of the Directive, however the principle remains valid in the context of 28 (4).


102 Google Spain, Case C-131/12, at par. 78.

103 Kuner, *The global reach of EU data protection law, supra*, (“The Court did not limit its holding to claims brought by EU individuals, or to search engines operated under specific domains. An individual seeking to assert a right under the Directive need not be a citizen of an EU Member State, or have any particular connection with the EU, as long as the act of data processing on which his or her claim is based is subject to EU data protection law under Article 4.”).
Restrictions, however, came a few months later through the Art. 29 WP guidelines. In that document, while the WP recognized that “[a]rticle 8 of the EU Charter of Fundamental Rights, to which the [Google Spain] ruling explicitly refers in a number of paragraphs, recognizes the right to data protection to ‘everyone,’” it declared that “[i]n practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State.”104 Beyond these two examples, however, the group does not elaborate on the specifics of what constitutes such a ‘clear link.’

Current practice under the RTBD has only served to muddle this issue further, as the search engines that are currently deciding these cases have not implemented the requirement in a cohesive manner. The search result deletion form instituted by Microsoft’s Bing, for instance, requires the claimant to confirm her ‘country of residence’ using a scrolling list of countries concerned by the RTBD.105 Strangely enough, the form does not mention nationality as a connecting factor, though it has been recognized by the Art. 29 WP guidelines mentioned above; it also expands the scope of the RTBD to residents of countries located outside of the European Union, such as Switzerland.106 Google’s request form is even more confusing as it does not ask to confirm the petitioner’s place of residence or citizenship but for the “the country whose law applies to [the] request.”107 Given that the place designated by the latter will not always coincide with the former,108 one may wonder if Google uses this term as erroneous shorthand, or if it considers application of a local data protection law to a given RTBD request as an actual limitative factor. The report by Google’s Advisory Council, which refers to asking “the data subject’s name, nationality, and country of residence,”109 seems to point towards the first of these possibilities, yet without providing a conclusive answer.

All in all, under the impulse of the Art. 29 WP, there seems to be a move towards requiring some link with the European Union before going forward with a RTBD claim though the specifics of this requirement are still obscure and vary in practice.

Application to the example cases
Applying the Art. 29 WP’s recommendations to case 6 yields the result that A2, being a Spanish national, will be able to file her RTBD request before European DPAs, even though her links with Spain are now tenuous at best. This is because the WP’s guidelines retain nationality as a sufficient connecting factor.

This result is unsatisfactory, because nationality and citizenship as connecting criteria do not take account of a person’s current and actual links with the European Union, allowing for forum shopping exercises such as the one envisaged in that case. Furthermore, the lack of guidance as to what constitutes a ‘clear link’ in the Working Party’s conception is to be deplored; especially since it has given rise to wildly divergent practices when it comes to RTBD claims addressed to search engines.

104 Art. 29 WP, Guidelines, supra, at 8.
105 Request to Block Bing Search Results in Europe, supra.
106 Id. Bing also offers its RTBD service to users located in Iceland, Liechtenstein, and Norway.
107 Search removal request under data protection law in Europe, supra.
108 See infra, at 40-41.
109 Google Advisory Council, supra, at 15.
**APPLICABLE LAW**

The preceding section has found that – barring some uncertainties – the Spanish DPA has authority over every foreign search engine envisaged in the present case study. However, in order for the corresponding claimants to effectively make use of the RTBD against them, it must also be found that the data protection law of a European Member State, and preferably Spanish law, applies to their serving of search results. This section will thus tackle three questions:

- Is the RTBD applicable to the activity of each of these search engines?
- If that is the case, which national data protection law applies?
- If multiple laws may find themselves applicable at the same time, which one is relevant for the purposes of deciding whether or not to remove search results?

The last two questions may seem rather theoretical at first blush, given that the RTBD is a tool of European data protection law that is applicable across all of the Member States’ laws. However, it is submitted that the analysis of which particular European law applies in any given case will prove itself as relevant in two respects. First, because, as seen just above, full jurisdictional powers over a foreign data controller are granted to DPAs depending on which law applies.\(^{110}\) Second, because the practice of the RTBD is still regionalized,\(^{111}\) determining which particular national data protection law applies thus determines how any given RTBD request will be handled.

**ARTICLE 4 (I) OF THE DATA PROTECTION DIRECTIVE**

The geographical scope of the Data Protection Directive is set out in its article 4, paragraph 1. It is formulated in the following manner:

Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable; . . .

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.\(^{112}\)

---

\(^{110}\) See *supra*, at 12-15, 21-22.

\(^{111}\) See *supra*, at 8-10.

\(^{112}\) The letter (b) of the provision, which contemplates situations in which “the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law,” being irrelevant to the course of the present analysis, will not be examined in the following section.
Letter (a) of the provision relies the presence of an ‘establishment’ of the data controller as its main connecting factor for the application of local data protection law; letter (c), which applies if letter (a) is not fulfilled – meaning that the data controller owns no establishment in any Member State – foresees the application of local data protection law if the data controller makes use of ‘equipment’ in for its processing a given Member State. The following section will examine how the provision works when applied to the example cases, first turning towards the letter (a), and then towards its letter (c).

**LETTER (A): THE LAW OF THE ESTABLISHMENT OF THE DATA CONTROLLER**

Under article 4 (1) (a) of the Data Protection Directive, there are three elements that must be examined in order to determine whether the law of a Member State applies to a data controller. There must be an act of data processing; its controller must have an establishment located on the territory of a given Member State; finally, the act of data processing must be carried out “in the context of the activities” of that establishment. All three conditions shall now be examined in succession.

**Data processing**

Much like article 28 (4) and (5) on DPA jurisdiction, article 4 (1) (a) targets acts of data processing as performed by their related data controller. Unlike those provisions, however, article 4 (1) (a) does not require identification of where that processing occurs in order to operate; instead, whether or not the data protection law of a given Member State applies depends on the other conditions – i.e. whether that processing can be attached to the activity of an establishment of the data controller, and whether that establishment itself is located in the territory of that Member State.

As seen earlier in the present paper, the acts of data processing specifically targeted by the RTBD are the operations related to a search engine’s activity as a provider of search results; these include the indexing of content found on the World Wide Web, the display of that content to end users, and the web crawling performed prior to the indexing. Since article 4 (1) (a) only puts weight on the nature of these operations as part of the activity of an establishment’s, there is no real need here to distinguish between them or to locate where they might take place, as has been the case in the context of the discussion surrounding DPA jurisdiction.

**Establishment**

Article 4 (1) (a) rests upon the principle that the main connecting factor leading to the application of a given national data protection law to a data controller is the presence on the territory of that Member State of an establishment. While the provision itself does not provide a definition of this term, recital 19 of the Directive states that “establishment on the territory of a Member State implies the effective and real exercise

---

113 Art. 29 WP, Opinion on applicable law, supra, at 19; Morel, supra, at 35; van Alsenoy, Kuczerawy, & Ausloos, supra, at 24. The exact implications of the relationship between the two letters of the provision are, however, not clearly defined; for more on this in the context of Google Spain, see infra, at note 139 and accompanying text.
114 Van Alsenoy & Koekkoek, supra, at 7.
115 Art. 29 WP, Opinion on applicable law, supra, at 12.
116 Supra, at 16-17.
117 By ‘establishment,’ it is not meant only the primary establishment of a data controller, but any secondary establishment. This has the effect of allowing European law to apply to data controllers headquartered outside of the European Union; on this point, see Morel, supra, at 96-97.
of activity through stable arrangements” and that “the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect.”

The term has been traditionally interpreted as requiring both a degree of permanence and a degree of activity. For example, according to the Art. 29 WP, the presence of an attorney office or even a single agent or representative, if found sufficiently stable, fulfills the criteria; by contrast, the presence of a web server or a computer which may display the website of the data controller, does not.118 Also of relevance is the ECJ’s uncontroversial finding in Google Spain that Google’s subsidiary in Spain, which acted as commercial agent in that territory, fulfilled the characterization.119

But what are the outer limits of the term ‘establishment’? Some guidance as to this point is again found in the ECJ’s Weltimmo decision, in which it had to face a decidedly tricky set of facts. Weltimmo s.r.o was a two-man company headquartered in Slovakia that operated a website offering real estate listings for properties located in Hungary. The company refused to honor requests emanating from some of its Hungarian advertisers asking for the deletion of their listings after the website’s free one-month trial period; instead, the company kept their listings, charged them for its service, and eventually forwarded their data to collection. The advertisers, in turn, filed a series of complaints with their local DPA. Though both of Weltimmo’s owners resided in Hungary, the company itself only owned a post box and a bank account in that Member State. One of the owners, however, acted in the name of the company in Hungary as an agent of debt collection and as a representative during the proceedings brought before the DPA.120 Among other questions – including a jurisdictional enquiry which has been already described earlier in this contribution121 – the ECJ had to answer whether these contacts were substantial enough to suggest that Weltimmo operated an establishment in Hungary, or if the fleeting nature of these contacts, and namely the fact that the owner’s activity as a representative in Hungary arose in part due to the dispute in question, precluded this conclusion.122

The Court started its answer on this point by considering that the definition of ‘establishment’ set out in recital 19 of the Directive, since it puts emphasis on the “effective and real exercise of activity through stable arrangements” and that, correspondingly, “the legal form of such an establishment . . . is not the determining factor,” results in a “flexible” definition, “which departs from a formalistic approach whereby undertakings are established solely in the place where they are registered.” “Accordingly,” the Court followed, “both the degree of stability of the arrangements and the effective exercise of activities in [a] Member State must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned.”123

When it came to companies offering their services exclusively through the Internet, such as in this particular case, the Court opined that the flexible character of the notion of establishment was to be emphasized.

---

118 Art. 29 WP, Application of EU data protection law to non-EU based web sites, supra, at par. 2.1; Opinion on data protection issues related to search engines, supra, at 10; Opinion on applicable law, supra, at 11-12.
119 Google Spain, Case C-131/12, at par. 49.
120 Weltimmo, Case C-230/14, at par. 13.
121 Supra, at 13-15.
122 Weltimmo, Case C-230/14, at par. 19.
123 Id., at par. 29.
Relying on that point on the arguments set out by Advocate General Cruz Villallón in his opinion, it considered that the situation of Internet companies, since they have the ability to bring their business to several jurisdictions at once through their online activities, relativized the need of creating a stable office or establishment in the traditional sense of the word. Even the deployment of a single agent equipped with a laptop in a given jurisdiction could fulfill the role of exercising stable arrangements in that place, provided that the company in question already directs its online business activity there.\textsuperscript{124} The Court then went on to find that “in the light of the objective pursued by [the Data Protection Directive], consisting in ensuring effective and complete protection of the right to privacy and in avoiding any circumvention of national rules, . . . the presence of only one representative can, in some circumstances, suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question.”\textsuperscript{125}

Applying this standard to the case at hand, the ECJ considered that since “the activity exercised by Weltimmo consists, at the very least, of the running of one or several property dealing websites concerning properties situated in Hungary, which are written in Hungarian and whose advertisements are subject to a fee after a period of one month,” there was ample evidence to suggest that it “pursues a real and effective activity in Hungary.”\textsuperscript{126} Furthermore, the company had “a representative in Hungary, who is mentioned in the Slovak companies register with an address in Hungary and who has sought to negotiate the settlement of the unpaid debts with the advertisers”; it also had “opened a bank account in Hungary, intended for the recovery of its debts, and [used] a letter box in that Member State for the management of its everyday business affairs”; taken all together, this was sufficient to consider that Weltimmo had an establishment in Hungary.\textsuperscript{127}

The \textit{Weltimmo} decision thus stands for the proposition that in cases involving data controllers doing business over the Internet, the requirement of having an establishment in a Member State for the purposes of applying local law under article 4 (1) (a) of the Directive will be easy to fulfill as long as that Member State is targeted by that online business activity. When considered from the point of view of the RTBD, \textit{Weltimmo} could imply that the presence of a single lawyer or business representative of a foreign search engine in a Member State may be sufficient as soon as the search engine does business – i.e. serves search results and advertisements – in that Member State.

\textbf{Processing performed in the context of the activities of an establishment}

In order for the national data protection law of a given Member State to apply to an act of data processing, it does not suffice to observe that the related data controller owns an establishment on the territory of that Member State; there is also a requirement of a factual link between the activity performed by this establishment and the act of data processing at hand. Following the terms of article 4 (1) (a), the processing must have occurred “in the context of the activities of [the] establishment.”\textsuperscript{128}

\begin{footnotes}
\item[124] \textit{Opinion of Advocate General Cruz Villalón, Weltimmo s.r.o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, Case C-131/12, Jun. 25, 2015, at pars. 35-36.}
\item[125] \textit{Weltimmo, Case C-230/14, at par. 30.}
\item[126] \textit{Id., at par. 32.}
\item[127] \textit{Id., at par. 33.}
\item[128] \textit{Art. 29 WP, Opinion on data protection issues related to search engines, supra, at 10; Opinion on applicable law, supra, at 12-17; Morel, supra, at 97-98, 100, 107-110.}
\end{footnotes}
This element of the provision serves two different roles. The first role is external in nature: depending on how a given activity of data processing may be thought of as falling into the ‘context of the activities’ of an establishment located in a Member State and owned by a data controller otherwise headquartered outside of the European Union, the standard determines whether or not European data protection law, as a whole, applies to this activity. The second role of the rule, conversely, is internal: by attaching an act of data processing to an establishment grounded in a specific Member State, it also determines which data protection law, out of those of all the Member States, applies to it. This second role of the rule is particularly important in situations in which the foreign data controller owns several establishments located in multiple Member States. In those cases, its attaching function will serve as a ‘tie breaker’ of sorts, designating which one of these establishments, and thus which data protection law, is responsible for every given act of data processing. It thus serves as a protection against conflicts between competing Member State laws and the risk of regulatory overlap.

Given the multiple dimensions of the rule, it follows that determining what exactly falls in the ‘context of the activities’ of an establishment is the central piece in determining the applicable law pursuant to article 4 (1) (a) of the Directive. The first part of this section will present how the ECJ applied the notion in the context of the RTBD in its Google Spain decision; it will be shown that the Court adopted a broad meaning of the term ‘context of activities’ in order to secure the application of European data protection law to Google. The second part of the section will then consider this finding from the point of view of the internal function of the rule, and will show that, due to the same broad approach adopted in Google Spain, this particular aspect is subject to many uncertainties.

**Google Spain and the ‘context of activities’**

One of the key issues in Google Spain centered on whether or not Google Inc.’s activity of serving search results, including the result that prompted González to file his original removal request with the Spanish DPA, was subject to European data protection law and, in particular, the Spanish data law implementing the Directive. While Google Inc.’s head office was (and still is) located in Mountain View in California, the firm had, since 2003, a physical presence in Spain through its Google Spain subsidiary, located in the city of Madrid. Google Spain, however, did not participate directly in the indexing, processing, and serving of search results; rather it acted as a commercial agent for Google in Spain and was mainly tasked with offering and marketing the sale of advertising space displayed on the search engine to local businesses.\(^1\) Given that Google Spain did exercise stable arrangements through this activity, the ECJ had no trouble, as mentioned in the previous section, in characterizing it as an establishment under article 4 (1) (a) of the Directive.\(^2\) Less clear, however, was the issue of whether Google’s serving of search results to end users located in Spain, i.e. the targeted act of data processing, fell ‘in the context’ of the commercial activities of Google Spain.\(^3\)

Unsurprisingly, Google argued that this was not the case. It invoked the fact that Google Spain played no role in the processing activities that gave rise to the display of search results; that its activity as a commercial agent was independent from that processing, and that while it did conclude deals with local firms regarding

---

\(^1\) *Google Spain*, Case C-131/12, at par. 46.

\(^2\) *Id.*, at par. 49.

\(^3\) *Id.*, at par. 50.
the display of advertisements alongside search results, that display was, from a technical standpoint, separate from the algorithms that rank and serve search results. The sole entity responsible for the serving of search results was Google Inc., therefore it could not be concluded that this act of data processing fell into the context of the activities of Google Spain.\(^{132}\)

Google’s insistence on a strict technological meaning of the term ‘in the context of’ went, however, against the views of earlier guidance from the Art. 29 WP. Indeed, in its 2008 opinion on search engines, the WP already had the opportunity of discussing the operation of article 4 (1) (a) of the Directive when applied to these operators.\(^{133}\) In that document, it considered that, in order for local law to apply, the establishment should “play a relevant role in the particular processing operation.” It then added that this was “clearly the case” when “the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data,” when “an establishment is responsible for relations with users of the search engine in a particular jurisdiction,” and when “a search engine provider establishes an office in a Member State . . . that is involved in the selling of targeted advertisements to the inhabitants of that state regard to user data.” While these three examples point to a broad reading of the requirement in general, the latter one suggests that Google Spain’s activities were indeed sufficiently linked to the processing of search results.\(^{134}\)

Reaching the same conclusion in his opinion on Google Spain, Advocate General Jääskinen highlighted that the finality of a search engine’s business model closely relates the display of search results with the capacity to conclude advertising deals with third parties.\(^{135}\) A search engine “normally relies on keyword advertising which is the source of income and, as such, the economic raison d’être for the provision of a free information location tool in the form of a search engine. The entity in charge of keyword advertising . . . is linked to the internet search engine” and it thus “needs presence on national advertising markets.” It is for this reason, he added, that “Google has established subsidiaries in many Member States” and that it “provides national web domains such as google.es or google.fi.”\(^{136}\) He then concluded that “the business model of an internet search engine service provider must be taken into account in the sense that its establishment plays a relevant role in the processing of personal data if it is linked to a service involved in selling targeted advertisement to inhabitants of that Member State.”\(^{137}\)

In its subsequent decision, the ECJ fully agreed with these views, stating inter alia that “the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.”\(^{138}\)

---

\(^{132}\) Id., at par. 51; see also van Alsenoy & Kockkoek, supra, at 7-8.

\(^{133}\) Art. 29 WP, Opinion on data protection issues related to search engines, supra.

\(^{134}\) Id., at 10; but see also Hardy, supra, at part III C. According to this author, the WP’s approach was less broad then the one of the ECJ in Google Spain, as it required that the establishment actually deal with personal user data – along with the display of advertisements, in order to fulfill the criterion.

\(^{135}\) This relates back to the two facets of a search engine’s business model, see supra, at 16-17.

\(^{136}\) Opinion of Advocate General Jääskinen, Google Spain SL v. AEPD, supra, at par 63.

\(^{137}\) Id., at par. 65.

\(^{138}\) Google Spain, Case C-131/12, at par. 56.
In addition to this argument, the Court was preoccupied by another issue, namely the fact that, if it were to decide that Google’s search engine would entirely escape the reach of European data protection law. Indeed, article 4 (1) (c) – the backup ‘long arm’ provision of the Directive – could not apply to the case since Google had establishments in the European Union, meaning that only 4 (1) (a) could be used as a gateway to submit Google to the principles of the Directive including the RTBD.139 “It cannot be accepted” the Court thus argued “that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive’s effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure.”140 Thus, it concluded that “an establishment such as Google Spain satisfies the criterion laid down in article 4 (1) (a) of Directive 95/46.”141

Branches or subsidiaries established by search engines in Member States in order to provide advertising space to local third parties are, following Google Spain, establishments liable to attract the application of European data protection law and in particular of the RTBD. Beyond this narrow conclusion, however, the decision leaves out two areas of uncertainty.

First, it remains unknown whether the goal of providing effectiveness to the principles of the Directive, invoked by the ECJ in its arguments, would dictate the same conclusion regarding other establishments that do not have a hand in the technical aspects of serving results, but do serve a relevant purpose for the whole of the search engine’s business. As mentioned above, the Art. 29 WP’s opinion on search engines foresees that the criterion would be fulfilled by a search engine’s legal representative, or by an outlet generally responsible for its “relations with users . . . in a particular jurisdiction.” Would it be possible to consider that the serving of search results occurs ‘in the context’ of a search engine’s legal office, or of one of its commercial representatives? Google Spain, along with the Weltimmo decision, which further opened up the definition of what passes for ‘establishment’ under the Directive, does seem to suggest so.142

Second, the ECJ’s finding in Google Spain creates uncertainty around search engines having establishments located in several Member States. This argument implies a consideration of the internal role of article 4 (1) (a) of the Directive, towards which this text shall now turn.

---

139 This risk was underlined in the Opinion of Advocate General Jäärkinen, Google Spain SL v. AEPD, supra, at par. 63, (“In this factual context the wording of Article 4(1) of the Directive is not very helpful. Google has several establishments on EU territory. This fact would, according to a literal interpretation, exclude the applicability of the equipment condition laid down in Article 4(1)(c) of the Directive. On the other hand, it is not clear to what extent and where processing of personal data of EU resident data subjects takes place in the context of its EU subsidiaries.”); contrast, however, with the interpretation set forth by the Art. 29 WP in its Opinion on applicable law, supra, at 12 (“Article 4(1)c will apply where the controller has an “irrelevant” establishment in the EU. That is to say, the controller has establishments in the EU but their activities are unrelated to the processing of personal data. Such establishments would not trigger the application of Article 4(1)”); see also Hardy, supra, at part III B; Morel, supra, at 103-106, Svantesson, supra, at p. 6-7.

140 Google Spain, Case C-131/12, par. 58.

141 Id., par. 59.

142 Fearing that the Google Spain precedent might be extended to allow for the application of local law to any kind of branch or subsidiary owned by a foreign Internet intermediary, see Tassis & Peristeraki, supra, at 251.
Multiple establishments

When a data controller owns several establishments located in different Member States, article 4 (1) (a) *in fine* states that it “must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.” The Directive thus stands for the principle that multiple national laws may apply simultaneously to the same data controller, as each of its establishments is bound to apply local law to the processing it performs. In order to avoid possible regulatory overlap, however, the requirement that local law may only apply if a given act of processing is performed ‘in the context’ of the activities of an establishment located in that jurisdiction operates as a *de facto* conflict rule, essentially distributing every act of processing to the sphere of activity of its relevant establishment.143

This internal role of the rule was recognized and emphasized by the Art. 29 WP in its 2010 opinion on applicable law. In that document, it recognized that “the multiplication of applicable laws is . . . a serious risk” and that “[t]o determine whether one or several laws apply to the different stages of the processing, it is important to have in mind the global picture of the processing activities,” before finding that “in such circumstances, the notion of "context of activities" – and not the location of data – is a determining factor in identifying the applicable law.”144

In order for this factor to perform its role of discriminating between different national data protection laws, the WP further opined that it should take on a robust character, accounting for the degree of involvement of the establishment in the data processing activities of its owner – e.g. whether it factually processes the data in the context of its own activities – and the nature of the activities at hand. In short, a functional approach of the notion of ‘context of activities,’ resting on a ‘who does what’ basis, should be followed in order to avoid confusion about what law applies to what activity.145

When viewed from this angle, the holding in *Google Spain* appears less desirable. To be sure, the display of search results rendered by Google may be placed in the context of the activities of Google Spain because of the latter’s relationship with its parent company’s overall business plan. Yet, with that subsidiary having no direct hand in the processing aspect, it may equally, and for the same reasons, be placed in the context of the activities of Google Copenhagen, of Google Paris, of Google Berlin, or of any of the 19 other subsidiaries owned by the company, located in the European Union and providing advertising space to third parties.146 Lacking a sufficient ‘who does what’ basis, the display of search results is potentially subject to the parallel application of the national data protection law of any Member State in which an establishment is present.147

Now, it could be argued that a contextual reading of the facts at hand in *Google Spain* may sidestep this issue. Since the case concerned a request emanating from a Spanish citizen, made in front of the Spanish DPA, and concerning a link leading to a Spanish newspaper reporting on events happening in Spain, Spanish data

143 Art. 29 WP, Opinion on applicable law, supra, at 9-10; Hardy, supra, at part III B; for more details on the history of the interpretation of the provision, see Morel, supra, at 97-98, 100, 107-110.
144 Art. 29 WP, Opinion on applicable law, supra, at 12-13.
145 Id., at 14-17.
146 Google locations, supra.
147 Hardy, supra, at part III D (in favor of a ‘closest connection’ or ‘center of gravity’ approach acting as a tie-breaker); Hayes, supra, (“On a literal reading of the Court’s findings, a German data controller, with all relevant data processing operations based in Germany, could find itself subject to French data protection law simply because it had a subsidiary engaged in promotional activities in France.”).
protection law, out of all other Member States, was certainly the most appropriate to regulate the proceedings. The fact that the case centered on search results offered to Spanish end users also pointed in that direction. However, article (1) (a) of the Directive does not permit the reliance on such a ‘center of gravity’ approach to select between the laws possibly applicable to an act of data processing. Whether this sort of analysis was possible was actually one of the questions posed by the referral court in Google Spain and rejected by Advocate General Jääskinen in his opinion.148 Furthermore, as explained above in the section devoted to jurisdiction, Mario Costeja González could very well have filed his request before the French or German DPA, where Google also displays results and owns establishments,149 what law would have applied then?

All in all, it is submitted that, through its interpretation of article 4 (1) (a) in Google Spain, the ECJ ensured that Google would be led to implement the RTBD; in the same breath however, it weakened the provision’s function as a tie breaker in internal multi-establishment cases. The uncertainty surrounding these situations will be underlined in the next section, where these rules will be applied to the example cases.

Application to the example cases

In case 1, the search engine B1 has its headquarters in California and owns multiple subsidiaries tasked with the management of local business affairs, such as the selling of advertising space; they are located in Spain, Ireland, and France. These subsidiaries are establishments for the purposes of article 4 (1) (a) of the Directive; subsequently, and following the ECJ’s holding in Google Spain, B1’s serving of search results in the European Union falls into the context of their activities. The Spanish, Irish, and French data protection laws may thus equally apply, with no clear way of presumptively deciding between them. In practice, it may very well be that this choice may be ultimately performed by claimant A1, who may choose to file her request in front of the DPA of any of these Member States, with the selected authority applying its national data protection law for simplicity’s sake.

In case 2, the search engine B2 owns only one establishment in the European Union, which is located in Ireland. It thus follows that all RTBD claims directed against it, and in particular the one contemplated by claimant A1, a Spanish citizen, will be examined under Irish data protection law.150 Following the jurisdictional rules set out in Weltimmo, only the Irish DPA will be able to impose fines upon B2.151 This solution is problematic, because there is no link between A1’s claim and Ireland except for the fact that B2 chose to place a subsidiary there. A1 would certainly prefer to have the Spanish DPA under Spanish data protection law decide whether or not the search results displayed by B2 harm her personality in such a way that they should be removed. This unwelcome result stems from the way article 4 (1) is structured: since its letter (c) only applies in cases in which the letter (a) does not apply; as long as a single establishment is present in any Member State, the law of that Member State will apply. Indeed, the Directive does not offer

149 supra, at 22.
150 Ustaran, supra, at 9 (discussing that, even in the context of the RTBD, “publicly appointing an EU-based entity as a data controller should still allow global businesses to operate across the EU whilst only being subject to the data protection laws of one member state.”)
151 supra, at 21-22.
a backup rule or an escape clause allowing for the application of the law of another Member State if the law of the place of the establishment appears as too remote in a given situation.

Case 3 presents a different kind of problem. Search engine B3 has no formal presence in the European Union; however two of its developers reside in France and work from their homes via teleconferencing. Two questions arise: is their presence sufficient to constitute an ‘establishment’? If that is the case, can it be said that the serving of search results occurs ‘in the context’ of their activities as developers? The first question rests on an interpretation of the Court’s opinion in Weltimmo: on the one hand, placing an establishment there would seem artificial even by that case’s standards, as those developers are neither representatives nor agents of the company and, in particular, they do not partake in any promotional activity directed towards French users of the search engine. Denying the presence of an establishment of B3 in Europe in this way would not, however, mean that the Directive would not apply at all to its activities as a search engine since letter (c) of article 4 (1) will then become applicable as a backup scope rule. On the other hand, it may be argued that search engine B3 directs its business – the display of search results alongside advertisements – in France and that the developers located there form a key part of its infrastructure. Then, following the holding in Google Spain, a finding that this display happens ‘in the context of’ their activities will become irresistible in order to avoid gaps in the scope of the Directive. This should then lead to the conclusion that French data protection law applies to all RTBD claims filed against B3.

Finally, case 6 allows for a consideration of whether the results obtained above would be any different if the claimant were not domiciled in Spain, but in Arizona, her only link with the legal order of the European Union being her Spanish nationality. Since article 4 (1) (a) does not in any way consider the personality of the recipients of the protections granted by European data protection law, this question will have to be answered in the negative.

**LETTER (C): THE LAW OF THE PLACE WHERE PROCESSING EQUIPMENT IS LOCATED**

**Standard**

Article 4 (1) (c) of the Directive states that a data controller that has no establishment on the territory of the European Union may still be subject to the data protection law of a Member State if, “for purposes of processing personal data,” it “makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.” Because the ECJ in Google Spain was satisfied that Spanish law applied to Google Inc. through its Google Spain establishment, it did not provide guidance as to how this provision should be interpreted in the context of the RTBD; the same can be said for the Art. 29 WP guidelines on the RTBD. Lacking any direct source, the following discussion will thus rely on the WP’s earlier work on the provision to elucidate its implications for foreign search engines.

---

152 For this side of the analysis, see infra, at 36.

153 Contrast the results obtained here, mutatis mutandis, with the options proposed in the case resolutions performed in Morel, supra, at 107-109.

154 Hardy, supra, at part III B.
As a first step, the provision requires the presence of equipment on the territory of a given Member State. The term ‘equipment’ is to be interpreted broadly and includes both human and automated means of processing, regardless of their size and shape; furthermore it is not required that the data controller control or own the equipment in question, as long as the latter is technically involved in the data processing at hand. This leads to the second step in the analysis, which requires that the equipment “is actually used to collect and process personal data” and which must be assessed on a case-by-case assessment. Central to this determination are two elements: the activity of the controller, and its clear intention of processing personal data through the equipment. If these conditions are fulfilled, then the data protection law of the Member State on the territory within which the equipment is located will apply to the whole of the processing operation, even if the particular processing performed by that equipment is but one step of the data processor’s entire activity. When envisaging the application of the provision to websites and search engines, the Art. 29 WP, emphasizing the need to avoid gaps in the application of the Directive, has usually interpreted it in a broad manner, considering for example that the placing of a cookie on an end user’s computer, by itself, fulfilled the criteria, that computer being the equipment targeted by article 4 (1) (c). That being said, the WP also recognized the need for foreign websites and search engine operators for foreseeability; at one point in its opinion on applicable law, it considered the possible addition of a targeting test to the provision, which would allow to take into account the operator’s intent to reach the public located at the place of the equipment. It did not, however, detail that thought any further.

Confronting article 4 (1) (c) with the RTBD leads back, in essence, to the discussion, already conducted in the realm of jurisdiction, of how and where the technical steps necessary to the processing of search results occur. Applying these developments mutatis mutandis, there are three places that could be alternatively characterized as the place where equipment is used for processing: the place of the servers where crawling is performed, the place where the data center performing the indexing operation is established, and the place where the end user’s computer displaying the search results is located. The third of these places falls without much trouble under article 4 (1) (c) of the Directive, as the display of search results on an end user’s machine fulfills the criteria of purposeful processing activity performed by an automated mean; furthermore, the WP has underlined that an end user’s computer falls squarely under the characterization of equipment. The second of these places would likewise not raise any significant problems of interpretation, however it is submitted that a search engine’s data center is closer in nature to the notion of establishment under art. 4 (1) (a) of the Directive, and that is should consequently fall under this rule rather than 4 (1) (c). Finally, the place of crawling, with that act being a data processing operation performed on a server, falls under the

155 Art. 29 WP, Application of EU data protection law to non-EU based web sites, supra, at 9; Opinion on applicable law, supra, at 20-22.
156 Id.
157 This issue is addressed in the Opinion on applicable law, supra, at 24 (“[T]he criterion of Article 4(1)c results in the principles of the Directive being applicable to the controller as such, for all the stages of the processing, even those taking place in a third country.”)
158 Art. 29 WP, Application of EU data protection law to non-EU based web sites, supra, at 10-12; Opinion on data protection issues related to search engines, supra, at 11 (“The use of cookies and similar software devices by an online service provider can . . . be seen as the use of equipment in the Member State’s territory, thus invoking that Member State’s data protection law.”)
159 Supra, at 20-22.
characterization; it does, nonetheless, raises the same issues of localization as when discussing jurisdictional matters.\textsuperscript{160}

**Application to the example cases**

In case 4, claimant A1 seeks to remove search results present on search engine B4, which is headquartered in the American State of California and owns no offices nor data centers in Europe; however, the search results it serves may be accessed from any Member State. Because each and every act of display of results can be characterized as ‘making use of equipment’ under article 4 (1) (c), subjecting the whole of B4’s search activity to the law of the location of that equipment, A1’s claim may potentially be regulated by any of the European national data protection laws, regardless of the other factual elements of the case. Since each national DPA would be equally justified in applying its local law to the claim, art. 28 (4) and (6) as interpreted by Weltimmo would then confer to each of them full jurisdiction over search engine B4, including the capacity to impose fines on it. A1 may thus shop for both the forum and the applicable law at the same time, selecting for example the French, German, and Polish DPAs at her convenience, whatever her personal links with these Member States may be. In terms of foreseeability for the search engine operator, this outcome is evidently deficient.

The same questionable results may appear if one were to apply article 4 (1) (c) to search engine B3, which serves its search results all across the European Union yet has no presence there beyond a few of its developers residing in France. Paradoxically enough, if one considered – as shown in the previous section\textsuperscript{161} – that these few developers were sufficient to constitute an ‘establishment’ under article 4 (1) (a), and that the serving of results was performed in the context of it, then French law, and only French law, would apply instead. Case 3 thus highlights a problem created by the relationship between letters (a) and (c) of article 4 (1); given how broadly article 4 (1) (c) could be interpreted in terms of scope, foreign search engines would better off creating a visible establishment in single Member State in order to attract a single applicable law – and to be subject to the full jurisdictional powers of a single DPA. From a broader perspective, one may also wonder why the characterization of a few developers as an establishment might have such large effects on the single question of whether Spanish claimant A1 might be able to remove a search result harming her privacy rights.

In case 5, search engine B5 does not own any establishments or data centers in the European Union and, in addition, makes use of geolocation technologies in order to avoid serving search results to users located there. However, in the course of its activities, it may have crawled and indexed content present on servers located in several Member States. Application of European data protection law will thus turn upon the question of whether it should be considered that crawling and indexing content on a server should be characterized as ‘making use of equipment’ in the sense of article 4 (1) (c); answering this in the positive, means – localization problems aside – that the law of multiple Member States would apply simultaneously to A1’s claim, much like in cases 3 and 4 above. This proposition, however, would unduly disregard search engine B5’s deployment of jurisdictional avoidance tools made precisely in order to prevent contact with the

\textsuperscript{160} Supra, at 20-21.

\textsuperscript{161} Supra, at 34.
legal order of the European Union; it would also remain blind to the fact that simply does not conduct its business there.

These case solutions show that a broad reading of article 4 (1) (c) results in the cumulative and sometimes unpredictable application of multiple Member State laws to the activity of foreign search engines. This is antithetical to the goal of the provision as the Art. 29 WP has underlined that it should respect the data controller’s need for foreseeability; in this sense, some thought should be given to the group’s proposition of adding a targeting requirement that would limit the application of local law to data controllers that clearly conduct business in the targeted Member State, so as to guarantee that the link with EU law “is effective and not tenuous (such as by almost inadvertent, rather than intentional, use of equipment in a Member State).”162 Such a proposition would handily solve case 5, where it is evident that search engine B5 does not conduct business in the European Union. However it may prove tricky to apply in situations similar to case 3 and 4, where the foreign search engine displays its results generally across Europe without making any distinctions between individual Member States.

COMMENTS AND ANALYSIS

COMPLEXITY, OBSCURITY AND INCONSISTENCY

Analyzing the case results obtained above from a general standpoint, it becomes apparent that the way in which the geographical scope of application of the RTBD is set out is flawed in multiple ways.

First, from a methodological perspective, it is excessively complicated. Identifying which DPA has jurisdiction for any given RTBD claim requires one to determine the contours of the targeted act of data processing and then define where it took place; this analysis demands some technical proficiency in how search engines work and requires an idea of where their data processing activities take place. Furthermore, knowing which DPA has the power to fine a given search engine requires an anticipated look into the question of which data protection law applies. Identifying this law, in turn, is no less challenging, as it requires one to hold an intimate knowledge of the functioning of article 4 of the Directive and to be able to apply it to the specific issue of the RTBD and of the processing of search results more generally. Should it be expected that the persons concerned by the RTBD, which are physical persons and search engines of all shapes and sizes, be able to conduct such an analysis just so that they may ascertain whether or not they fit under its geographical scope? Furthermore, should it be expected that all foreign search engines – with many of them being startups and only having a limited access to knowledge about EU law – be aware of the minute details of the scope of the 1997 Directive so that they may foresee if and how the RTBD applies to their business? It is submitted that these questions should be answered in the negative, and that the geographical scope of application of the RTBD should be expressed through a set of ad-hoc consistent set of bright-line rules instead of a complex renvoi to the basic scope rules of the Directive.

162 Art. 29 WP, Opinion on applicable law, supra, at 24; in this sense see also van Alsenoy, Kuczerawy, & Ausloos, supra, at 26 (data collection performed by crawling involves no determination about which data is collected, thus falling short of the ‘making use’ of equipment standard).
Second, not only is the geographical scope of the RTBD difficult to manipulate, it is also unsettled on many points due to the lack of attention to this topic on the part of both the ECJ and the Art. 29 WP. Is web crawling an act of data processing relevant for the purposes of establishing jurisdiction under article 28 (4) of the Directive and of establishing the application of local law under the ‘use of equipment’ standard of article 4 (1) (c)? If that is the case, how should its geographical localization be defined? If not, how should these rules be interpreted instead? How can one define which national law applies to the serving of search results when the search engine owns multiple establishment located in different Member States under article 4 (1) (a)? What exactly constitutes a “strong link” with the legal order of the European Union that the Art. 29 WP requires from a claimant in order to file a RTBD claim? Apart from establishing that the RTBD applies to Google through article 4 (1) (a), the Court and the Working Party have thus far failed to address the many uncertainties resulting from the juxtaposition between the traditional scope rules of the 1997 Directive and the very specific set of rights and obligations they have established under the RTBD. Needless to say, this situation does not provide any sort of stability or foreseeability to the recipients of the right and should, as such, be clarified.

Third, now going beyond these formal uncertainties, the results obtained through the case analysis performed in this paper suggest that that the geographical scope of the RTBD is unstable and inconsistent. This is firstly evident if one compares the solutions obtained in cases 1, 2, 3, and 4. All are variants of the same basic situation in which a Spanish national wishes to remove search results made available all over Europe by a search engine based in California. Depending on whether the search engine owned establishments in one or several Member States, it was alternatively found that one, or several, or all of the national data protection laws of the European Member States applied to that same claim, with no clear way of distinguishing between them. The results of cases 3 and 4 are especially unsatisfactory in this regard. The search engines in those cases held the least contacts with the European Union since they owned no establishment there. Yet, due to article 4 (1) (c) of the Directive being applicable since the letter (a) was not, the laws of every Member State in which end user computers were used as equipment to display search results were found to be alternatively applicable, meaning that the RTBD claim could be possibly be supported by the data protection law of any Member State. And since full DPA jurisdiction, including the right to impose fines, is justified by application of the *lex fori* following the *Weltimmo* rule, the claimants in those cases were found to be able to file their claims in each and every Member States of the European Union even though the targeted search engines owned no offices and had, in particular, not deployed any legal representatives on European soil. This result is made even more counterintuitive in case 3, in which some of the search engine’s key developers worked via teleconferencing from their homes in France, as finding that this presence would be sufficient to qualify as an ‘establishment’ under 4 (1) (a) would instead concentrate all RTBD litigation in France and under French law. Also questionable, though for other reasons, are the results obtained in case 5. In this one, the search engine did not even allow its content to be displayed in any Member State; yet depending on whether crawling and indexing could be included under the umbrella term of ‘processing’ under the Directive, it was found that it was still possible to subject it to the RTBD under the laws of multiple Member States and under the authority of their related DPA depending on the location of the servers it had indexed. Finally, case 6 highlights another issue since it was found that a Spanish person living in the State of Arizona could be protected by the RTBD even though she had no other relationship with the legal order of the European Union other than her nationality.
Taking all of these wildly diverging results together, one may wonder how any foreign search engine or physical person is supposed to foresee how and under what terms the RTBD applies to their situation. The answer is that they simply do not. As mentioned earlier, the large search engines that currently allow persons to file RTBD claims – Bing, Google, Yahoo! – allow claimants to select the DPA and the applicable law at the same time by a declaration of their home state, resulting in a de facto home country rule that does not take into account the actual geographical scope rules of the Directive. As for smaller search engines, such as Duck Duck Go – the situation that inspired case 3 of the present exercise – they do not implement the RTBD at all, though they technically should given the broad scope described above. Right now, these issues are overshadowed by the fact that Google occupies most of the landscape of the RTBD, but if the situation were to ever change, it is not impossible that the rules may break down.

SQUARE PEGS AND ROUND HOLES: THE RIGHT TO BE DELISTED V. THE DATA PROTECTION DIRECTIVE

At this point in the discussion, it might be tempting to pin all of these misgivings – complexity, unforeseeability, and inconsistency – on the fact that the Data Protection Directive was drafted in 1997 and that its scope rules were not made to accommodate digital undertakings. While this aspect certainly plays a role, it is instead suggested that there exists a more fundamental problem underlying all of this, namely, that the very framework relied upon by the Directive to define its own geographical scope simply does not work well when applied to the RTBD. On the one hand, the Directive is preoccupied with determining which national data protection law applies to the activity of data controllers as a whole, with the goal of subjecting that activity to the principles and obligations it contains; its scope provisions rely on identifying when and where processing occurs and on linking the identified activity to the entity responsible for it. On the other hand, the RTBD is the expression of an eminently personal right to data stewardship and privacy provided directly to physical persons; it takes the form of a series of one-time individual claims, each being filed by a different interested person and made against a specific act of release of personal data – that is the serving of a search result leading to either old, outdated or irrelevant information. Traces of this tension between the structure of the Directive and the goals of the RTBD have appeared throughout the results obtained in the present study.

The most obvious hint of it relates to the question of how the claimant is considered in RTBD cases. While dealing with case 6, in which the claimant had no link with the European Union besides her Spanish nationality, it was shown that the Directive takes, by design, the standpoint that all data subjects equally benefit from data controllers being subject to its principles; consequently, the personality of a claimant bringing a complaint before any DPA does not matter, which is evidenced by art. 28 (4) declaring that ‘any’ person may do so. This position is at odds with the RTBD, which is on the contrary deeply connected to the privacy rights, and thus the personal situation, of each and every claimant wishing to remove a search result bearing their name. Deciding whether or not a RTBD claim succeeds, according to the guidelines

---

163 Art. 29 WP, Opinion on applicable law, supra, at 7 (“The identification of applicable law is closely connected to the identification of the controller and its establishment(s): the main consequence of this link is the reaffirmation of the responsibilities of the controller, and its representative if the controller is established in a third country.”) Traditional cases used to frame the geographical scope of the Directive typically involve the question of what national data protection law applies in general to the data controller’s upkeep of a given dataset or database, for example, employee or client personal data; see for example Morel, supra, at 101-106.
drafted by the Art. 29 WP, depends on factors of substantive privacy law with most of them being linked to the claimant’s personality, how the linked content affects it, and how her interest in taking it down compares to the public interest of having that information available. These are questions like this: is she a public figure? Is she a minor? Is the information she seeks to remove accurate? Is that information relevant to her public, rather than private, life? What was the context of the original publication and what is its relevance regarding this person’s role in society? So on and so forth.\footnote{Beyond the criteria of the Art. 29 WP guidelines, see Ahmed, supra, at 183 (“While adjudicating a "removal request", three factors need to be taken into account: the first factor is time, as in when and how long ago was the information published; secondly, the impact of public accessibility to the information, basically the adverse effects the information has on the data subject at present; and lastly, the relevance of the information on the individual’s life, as in whether the information in question is of any present use to the individual or to the society with which he or she interacts . . . The principal goal of the RTBF is to avoid distortions of decisions that are made, taking into account aspects of the complete history of an individual, which may include events that are irrelevant or out of context.”).} This framework suggests that the RTBD is as much about the claimants making use of this protective right as it is about the interests of search engines bound to implement it and the interests of the public at large of having a right to information.\footnote{Noting this tension, see Hayes, supra, ("[The RTBD] essentially involves DPAs making decisions about what true and public information people are entitled to access online. One must seriously question whether such a regime, which could be construed as a form of censorship, was the intended purpose of the Data Protection Directive when it was adopted in 1995."); indeed, solutions proposed by scholars regarding the criteria of the RTBD are usually couched in terms of substantive privacy law, see, inter alia, Jones, supra, at 146-155 (suggests a reliance on existing speech laws to introduce a sort of RTBF in the US); Rustad & Kulevska, supra, at 399-416 (relying on a comparative analysis of national substantive privacy and defamation law to craft a harmonized RTBD proposal); van Als loosoy, Kuczeraw, & Ausloos, supra, at 46-58 (placing the RTBD within the ambit of Article 10 of the European Convention of Human Rights, promoting freedom of expression, and opposed to the right to privacy granted by the second paragraph of that provision and by the Data Protection Directive).}  These goals clash with the Directive’s main focus on the person of the data controller. It is rather telling that the Working Party, in the same guidelines, was compelled to limit the scope of the RTBD to persons having a ‘substantial link’ with the EU, thus adding in the same breath a personal scope limitation not present in the Directive itself.\footnote{Supra, at 23-24.}

Another hint of this tension can be found in the Directive’s reliance on ‘data processing’ as a connecting factor; this is the case in both jurisdiction under article 28 (4) and when determining applicable law under the ‘equipment’ standard of article 4 (1) (c). When contemplating the interests at stake regarding RTBD claims – as explained just above, the personality rights of the claimant against freedom of speech and information – it does not seem clear why the location of a server, a data center, or a user computer performing a technical operation is relevant for deciding which DPA has authority to assess individual claims for link deletion and which national law underlies that claim. The criterion is, it is conceded, generally useful for avoiding gaps in the Directive’s geographical scope, yet when applied to the case-by-case defendant-focused nature of the RTBD, it falls apart: not only does it bring unneeded complexity to the analysis by requiring one to assess where search results occur on a technical level, but it also leads to bad results. This is exemplified by the results of case 5, in which a search engine has chosen to avoid serving its content to European users, yet was found to be possibly subject to the Directive since it may have crawled servers located in one or several Member State(s).\footnote{Supra, at 22, 37-39.}

Similar criticism may be levied against the ‘establishment’ connecting factor used by the Directive to determine applicable law under article 4 (1) (a). As evidenced by case 2, a foreign search engine having an
establishment located in a single Member State is subject to the law of that state only, even if a Spanish claimant wishes to remove a link leading to a Spanish publication detailing her past demeanors in Spain. This, again, does not make much sense, as probably the Spanish DPA and law are more relevant to the case at hand and is further evidence that the nature of the Directive as a general framework for data protection, addressed mainly to data controllers in order to allow them to shape the course of their activity, clashes with the more personality-focused nature of the RTBD.

These elements show that, rather than focusing on processing or establishments, the locus of the RTBD should be determined in accordance with its stated goals – that is the protection of personal privacy and reputation against the publishing of harmful content. And while this submission seems challenging at first, the next section will demonstrate that not only did the ECJ state the RTBD in similar terms in its Google Spain decision, but that it also already hinted at its ideal locus, that is the place of the harm.  

**GOOGLE SPAIN REVISITED: THE RIGHT TO BE DELISTED AS A DESTINATION-BASED PERSONALITY HARM**

Earlier in the present paper, it was mentioned that the ECJ in Google Spain placed the RTBD firmly into the language of the Directive by referring to the whole of a search engine’s operations as data processing. That much is true: for example, when discussing whether or not the display of search results falls into its personal scope, it found that: “[I]n exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine ‘collects’ such data which it subsequently ‘retrieves’, ‘records’ and ‘organises’ within the framework of its indexing programmes, ‘stores’ on its servers and, as the case may be, ‘discloses’ and ‘makes available’ to its users in the form of lists of search results,” that “[a]s those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as ‘processing’ within the meaning of that provision,” and that, it “[i]s the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the ‘controller’ in respect of that processing pursuant to Article 2(d).”

The Court could have very well have stopped there. Yet, in the same section, it felt compelled to add the following observation: “Moreover, it is undisputed that [t]he activity of search engines plays a decisive role in the overall dissemination of [personal] data in that it renders the latter accessible to any internet user making a search on the basis of the data subject’s name, including to internet users who otherwise would not have found the web page on which those data are published.”

Further considering the role of search engines in civil society, it then went on to state that “the organisation and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users’ access to that information may, when users carry out their search on the basis of an

---

168 Reaching the same conclusion through a public international law analysis, see van Alsenoy & Koekkoek, supra, at 11-13; more generally, see also McNamee, supra, (calling Google Spain a move towards a “defamation like” vision of data privacy); Tassis & Peristeraki, supra, at 252.
169 Supra, at 17.
170 Google Spain, Case C-131/12, at par. 28.
171 Id., at par. 33.
172 Id., at par. 36.
individual’s name, result in them obtaining through the list of results a structured overview of the information relating to that individual.” These terms suggest that what the Court was really getting to is not the whole of a search engine’s processing activity, but rather the effect it has upon privacy rights by providing access to organized links harboring personal data to a potentially wide number of end users located across several Member States. Here, the strictly processing-oriented rationale contained in the Directive gives way to a more destination-based assessment.

The same language is relied upon by the Court when it moves on to the substantive part of its decision. This is the case for instance when it discusses how and why the Data Protection Directive imposes upon search engine providers the obligation of deleting outdated or irrelevant search results: “[t]he processing of personal data . . . carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual’s name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet — information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty — and thereby to establish a more or less detailed profile of him.” Right afterwards, the Court goes on to consider that “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.” Again, the language here seems to focus more on the impact that a search engine’s act of publication harbors for a person’s rights, rather than on the nature of the data processing operations allowing for this publication to be possible in the first place.

The Court’s most definite statement in that direction, however, lies directly within the operative part of the judgment. When describing the RTBD as an obligation under the Directive, it stated that “the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person’s name links to web pages, published by third parties and containing information relating to that person.” In other words, the RTBD only operates when a search engine displays its result list to end users, and even then, the removal only occurs following searches bearing the name of the claimant. A contraria, this means that the RTBD does not affect a search engine’s capacity for crawling and indexing pages present on the World Wide Web, nor does it affect its activity of ranking and serving these pages for all searches that are not connected to a person’s name. In truth, the RTBD is not really about how search engines process the personal data they retrieve from the World Wide Web, but is more about how they have the capacity of

173 Id., at par. 37.
174 Id., at par. 80.
175 Id., at par. 88.
creating a negative impact on a person’s fundamental right to privacy following the publication to the public at large of old or embarrassing information.

The Art. 29 WP guidelines only serve to reinforce this reading. It is true that, on its head, the document states that the RTBD is “an obligation of results which affects the whole processing operation carried out by the search engine”; yet it declares immediately afterwards that the right’s “adequate implementation . . . must be made in such a way that data subjects are effectively protected against the impact of the universal dissemination and accessibility of personal information offered by search engines when searches are made on the basis of the name of individuals.”176 The guidelines also underline that “the ruling expressly states that the right only affects the results obtained on searches made by the name of the individual and never suggests that the complete deletion of the page from the indexes of the search engine is needed. The page should still be accessible using any other terms of search.”177 It is also interesting to remark that, when discussing whether or not website specific search boxes should be included in to the personal scope of the RTBD, the WP relied on a pure impact-based assessment. Answering this question in the negative, it argued that they “do not produce the same effects as “external” search engines,” and that they “only recover the information contained on specific web pages . . . [E]ven if a user looks for the same person in a number of web pages, internal search engines will not establish a complete profile of the affected individual and the results will not have a serious impact on him.”178 The nature of the RTBD as focused on the harm occurring at the location of the end user consulting the website is, here, rather clear.

**PROPOSALS**

From the discussion conducted above, it can be concluded that the Directive’s geographical scope provisions – relying mainly on the identification and localization of the activity of the data controller – are a poor fit for the RTBD; and as evidenced all throughout this study, they simply do not yield good results. The nature of the RTBD as a subjective right allowing European citizens and residents to take down links leading to content harming their personality rights and thus allowing them to prevent these links from being displayed or published to end users, along with the sort of analysis it demands on a case-to-case basis – essentially pitting personality rights against freedom of speech and the right to information – suggests instead to take inspiration from how private international law has defined the geographical scope of personality and privacy torts; in that context, the main connecting factor used to determine both jurisdiction and applicable law is the place of reputational harm.179 With this in mind, and also taking into account all of the developments presented thus far, a series of proposals may now be presented.

---

176 Art. 29 WP, Guidelines, supra, at 9.
177 Id.
178 Id., at 8.
179 In the US, see *Calder v. Jones*, 465 U.S. 783 (1984), and Restatement (Second) of Conflict of Laws § 150 (2) (Am. Law Inst. (1971)) (“When a natural person claims that he has been defamed by an aggregate communication, the state of most significant relationship will usually be the state where the person was domiciled at the time, if the matter complained of was published in that state.”); in the EU, see *Regulation No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast)*, Official Journal of the European Union, L 351/1, Dec. 20, 2012, article 7(2), and the latter provision’s interpretation by the European Court of Justice in *Shevill v. Presse Alliance S.A.*, European Court Records 1995 p. I-00415, Mar. 7, 1995, and *eDate Advertising GmbH*, supra. As mentioned in note 55 of this paper, choice of law is not harmonized yet for these torts in European Law, however national law on that point
JURISDICTION

When it comes to jurisdiction, the ‘place of processing’ connecting factor used by article 28 (4) should be streamlined and slimmed down to include only two situations in which the DPA of a given Member State may have authority over a foreign search engine concerning RTBD claims.

The first one is when a Member State is the possible place of harm done to the claimant by the display of embarrassing or irrelevant search results in that Member State. This implies that it must be found that the search engine effectively offers its services as a search provider to end users located in that Member State; consequently no jurisdiction should be found if it has deployed technical means of blocking these users or otherwise avoiding contact with that territory. In order to protect the claimant’s interest of having an effective protection scheme for her personality rights, but also in order for the jurisdictional standard to remain easy to apply, it should not be required to show that the specific search result targeted for deletion has been published in that Member State, nor should jurisdiction hinge on whether or not the foreign search engine intended to ‘target’ this Member State as part of its business activity. On the other hand, in order to avoid forum shopping, jurisdiction should be conditional to evidence that the claimant holds an existing relationship with the legal order of the European Union. This will be the case if her domicile or habitual residence is located in a Member State or, barring that, if she manages to prove that she has a center of interests, for example due to familial contacts, there. If the claimant has filed her claim in front of a DPA located in another Member State than the one housing her connections to the European Union, then jurisdiction should still be retained; in this situation, then, the Weltimmo distribution rule will work in tandem with the law-selecting rules exposed below to allow for transfer of the case to the most suitable DPA.

Under article 28 (4) of the Directive, if the foreign search engine does not serve search results in the forum Member State, jurisdiction might still be appropriate if the search engine owns a data center there. This rule could be extended to cover all types of establishments, thus allowing for a more agreeable interplay between jurisdiction and applicable law under the Directive. Reliance on this connecting factor use should, however, remain confined to cases in which the search engine, while not directly displaying its results in the forum Member State, sought to avail itself of the business of the public located there in other visible ways.

APPLICABLE LAW

Turning towards choice of law, a first, ideal de lege ferenda proposal, which would see the RTBD’s law-selecting principles becoming unbound from the rules of the Directive, will be proposed. Then, a more modest de lege lata contribution, consisting of a series of suggestions on how to adapt the contours of article 4 to better suit the goals of the RTBD, will be provided.

Given the numerous pitfalls and complexities befalling article 4 of the Directive when applied to the RTBD, it would be indeed be ideal to entirely do away with it and to select the law applicable according to a place

agrees on a place of harm standard; for a thorough discussion see Reymond, supra; for a shorter piece from the same author proposing a jurisdictional solution for online torts, see Jurisdiction in case of personality torts committed over the internet: a proposal for a targeting test, 14 YbPIL 205 (2013).

Contrast with the proposal made by the present author in Jurisdiction in case of personality torts committed over the internet, supra. In this context, a targeting text was deemed necessary in order to provide a degree of foreseeability of the forum to all defendants in online privacy and defamation cases, as these persons may range in stature from individual private bloggers to larger press corporations. The RTBD, being addressed solely towards commercial search engines, does not require such modulation.
of harm standard. Under this construction, the applicable law to a RTBD claim would be the law of the place of the claimant’s habitual residence, provided that it is located in a European Member State and that the search engine serves its results there. Failing that, the place of the claimant’s domicile or center of interests could be used instead, provided that the same conditions are fulfilled.\footnote{For some inspiration on the idea of ‘center of interests,’ see \textit{eDate Advertising GmbH}, Cases C-509/09 and C-161/10 \textit{supra}, at pars. 48-50.} If the claimant has no substantial link with any Member State, or if the search engine operator has avoided contact with the European Union altogether, then the claim should naturally fail; these kinds of situation, however, should already be handled at the jurisdictional step as explained above.

The proposed standard is, admittedly, a home country rule. Yet it is simple, easy to apply, and it fits with the RTBD’s role as a tool of personal privacy protection. It avoids the current gaps and inconsistencies that exist due to the relationship between letter (a) and (c) of article 4 of the Directive, while also ensuring that only a single law will apply to a individual RTBD claim. It fulfills the ECJ’s goal, stated in \textit{Google Spain} and \textit{Weltimmo}, of guaranteeing a broad geographical reach to the RTBD, without having to deal with the many interpretative uncertainties left in the wake of these two decisions. It is also foreseeable for search engines, since these operators will be able to carve out from their services any jurisdiction or Member State home to laws they may wish to avoid. Finally, it corresponds to the current practice of the RTBD, which routinely sees claimants selecting their home data protection law when submitting removal requests to search engines.\footnote{\textit{Supra}, at 8-10 and 39.}

Such a proposal would however imply that the RTBD be separated from the geographical scope rules of the Directive; realistically, this does not seem probable: since the RTBD will be replaced in a couple of years by the possibly larger Right to be Forgotten contained in the GDPR, the chances of it gaining a legal standing of its own during this time period are rather slim. In the meantime, though, a more plausible prospect would be to interpret article 4 in such a way that the geographical scope of the RTBD may be manipulated in a more focused and consistent manner. Such a proposal seems especially plausible since the Art. 29 WP in its guidelines on the RTBD, has already started to tamper with the rules of the Directive to fit this nascent right.\footnote{\textit{Supra}, at 24-25.}

Regarding article 4 (1) (a) and the notion of establishment, it is submitted that, in order to fulfill the ECJ’s goal of avoiding gaps in the application of the Directive, the holdings of both \textit{Google Spain} and \textit{Weltimmo} should be retained, meaning that the presence of an advertising branch or subsidiary or even of a single representative on the territory of a Member State should be sufficient to constitute an establishment there as long as it can be demonstrated that the search engine provides its services to users located in that place. If the search engine owns establishments located in multiple Member States, then, if possible, the law of the Member State in which the claimant has her habitual residence, domicile, or center of interests should take precedence and apply to the RTBD claim as a whole. The most difficult situation arises if the search engine owns an establishment in one or multiple Member States in which the claimant has little or no personal link, as article 4 (1) (a) does not include a closest connection escape mechanism. One option would be, if possible, to select the law of the Member State that is the closest to the situation at hand within the constraints of the
establishment connecting factor; one other possibility would be to allow the search engine to agree to the application of the law of the claimant’s home state.

If no establishment is found, then article 4 (1) (c) will apply. It is here suggested that its ‘use of equipment’ standard should be interpreted as solely designating the place of display of search results, if the claimant has a reputation in that place. This would essentially bring it in line with the above proposed reading of article 28 (4) in the jurisdictional context, and will handily prevent the application of local Member State law to a foreign search engine over purely technical operations such as the crawling of websites hosted on servers located there.

CONCLUSION

The starting point of this contribution has been, all in all, a rather simple question of extending the rules forming the Right to be Delisted to search engines that are not Google. Yet, it led to major findings: on a micro level, this study has shown that the geographical scope of the right is complex, unstable, and fails to provide a consistent framework upon which stakeholders – physical persons and search engines alike – may rely. It has also shown that the way in which this right was instituted – and most notably by its concentration towards Google as its main gatekeeper – has only served to obscure these issues. On a macro level, it has raised a more fundamental question about the characterization of the Right to be Delisted as a legal notion sitting uneasily between, on one hand, its origins as a tool created under the framework of Directive 95/46/EC on Data Protection, and, on the other hand, its nature as a personal privacy shield against the republication of unwanted information.

The proposed General Data Protection Regulation, which at the moment of this writing is set to enter into force in a couple of years from now, will have the effect of concentrating European data protection under a single set of standards and practices. This should solve some of the micro issues identified in this paper; however, on the macro front, it remains to be seen whether the harmonization of data protection law in Europe will necessarily lead to a unified standard of the personal privacy elements that come into play when determining whether or not a link should be removed.184 On that point, one look at the work conducted under the Rome II regulation – and how the Member States have repeatedly failed to agree on a harmonized conflict of law rule for privacy torts – suggests that the road awaiting this future Right to be Forgotten, will be a bumpy one indeed.185

---

184 See Jones, supra, at 130-131 (underlining that the GDPR does not provide guidance on these points) and 167 (suggesting that the harmonization of privacy and free speech laws through the RTBF or the RTBD is not only unwanted, but politically and practically infeasible). Illustrating this challenge, and with much vigor, see Sébastien Proust, The proposed European Regulation on the right to be forgotten, or an end to national laws on the freedom of press, 24 Ent.L.R. 207 (2013) (“In democratic countries, freedom of the press—typically taken to mean the right of anyone, from journalist to blogger, to publish information (including information about other people)—is generally only subject to two main restrictions: defamation and breaches of a person’s right to privacy . . . So how it is possible for the proposed new EU regulation on personal data to endanger the cardinal principles of national press laws—in some cases centuries-old—without raising a public outcry?”).

185 Supra, at note 55.