

A critical analysis of the EU right to erasure as it applies to internet search engine results

Candidate number: 8019
Submission deadline: 1 December 2014 (Autumn Semester, 2014)
Number of words: 17960
Supervisor: Tobias Mahler



Table of contents

1	INTRODUCTION	1
2	PART A – AN INTRODUCTION TO DELINKING.....	2
2.1	Privacy and other fundamental rights in the EU.....	2
2.2	The idea of a right to erasure	3
2.3	The right to delinking	4
2.3.1	How a search engine works.....	4
2.3.2	The different contexts in which delinking can be pursued	5
2.3.3	Why pursue delinking from search engine results?	6
3	PART B – OVERVIEW OF THE EU RIGHT TO DELINKING	7
3.1	The DPD and the decision in <i>Google Spain</i>	7
3.1.1	The basis for the dispute in <i>Google Spain</i>	7
3.1.2	Procedural history	8
3.1.3	Judgment – first issue – the ‘territorial scope’	8
3.1.4	Judgment – second issue – ‘processing’ and ‘controller’	9
3.1.5	Judgment – third issue – the scope of the right to delinking.....	10
3.1.6	Summary of the position under the DPD	11
3.2	The GDPR	11
3.2.1	Outline of Article 17 – a right to erasure	13
3.2.2	Article 17 and search engine results.....	13
3.2.3	Summary of the right to delinking under the GDPR.....	18
4	PART C – A CRITICAL ANALYSIS OF THE RIGHT TO DELINKING	19
4.1	Criteria for assessment – privacy, freedom of expression and intermediary liability	19

4.2	Balancing the competing interests	22
4.2.1	Google on a tightrope	22
4.2.2	Should Google be the ringmaster?	34
4.3	Search engines and “controllers”	36
4.3.1	Can a SEO comply with the obligations on controllers?	37
4.3.2	Is it appropriate to treat a SEO as a controller?	38
4.3.3	Interim conclusion on the controller question	40
4.4	Extra-territoriality and non-EU search engines	41
4.5	Economic considerations	45
5	CONCLUSION	48
6	TABLE OF REFERENCE	50

ABBREVIATIONS

AG	Advocate General Jääskinen
Charter	Charter of Fundamental Rights of the European Union
Council	Council of the European Union
DPD	Date Protection Directive
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECtHR	European Court of Human Rights
EU	European Union
GDPR	Proposed General Data Protection Regulation
SEO	Search Engine Operator
TFEU	Treaty on the Functioning of the European Union

1 INTRODUCTION

In *Pride and Prejudice*, Jane Austen's character Elizabeth Darcy offers the following advice:¹

You must learn some of my philosophy. Think only of the past as its remembrance gives you pleasure.

In the digital age, Elizabeth Darcy's philosophy has become increasingly hard to abide by; with vast amounts of personal information online, readily accessible by a simple search engine enquiry of a person's name, for many it is impossible to escape the omnipresent intrusion of the internet into their private lives.

As a means to temper this digital threat, the EU has recently recognised a qualified legal right whereby a person can require a SEO to remove (delink) certain search results that would otherwise be displayed in response to a particular search enquiry (hereafter referred to as a "right to delinking"). This paper critically examines the operation of this right as it applies to truthful, legally published personal information on websites that are publically available and accessible through search engine results.

Several demarcations have been made to the discussion. Although it is acknowledged that a right to erasure might arise with respect to other functions provided by SEOs (such as 'autocomplete'), the present discussion is limited to the right to delinking.² Furthermore, as the focus is on delinking of *legally published* information, it is assumed that dissemination of that information cannot be restrained by the application of other legal doctrines such as contract, defamation, copyright, confidentiality or criminal law. Finally, the discussion concerns information that is *publically available* online. Therefore, the paper does not con-

¹ Austen, Jane, *Pride and Prejudice* (1853, RD Bentley), p323.

² Regarding autocomplete, see: Stuart, Allyson, 'Google Search Results: Buried if not Forgotten' (Spring 2014) 15(3) *North Carolina Journal of Law & Technology* 463, p480-481; Alsenoy, Van, Aleksandra Kuczerawy and Jef Ausloos, *Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?* (ICRI Research Paper 15, University of Leuven, 6 September 2013), p39-40.

sider the right to erasure with respect to personal information surreptitiously gathered by websites or search engines.³

The paper is structured in three parts. Part A provides a general introduction to the concepts that underpin the substantive analysis. Part B contains an outline of the right to delinking in the EU. The section sets out the current position under the DPD⁴ following the seminal decision in *Google Spain*,⁵ and interprets the likely future position under the GDPR.⁶ Part C provides the central discussion of the paper; a critical analysis of the right to delinking. This analysis is split into four areas; whether the framework appropriately balances the conflicting fundamental rights that are involved; the problems that arise from treating a SEO as a controller; the extra-territorial implications of the right; and the potential economic concerns. The paper submits that, on balance, there are significant concerns with the operation of the right to delinking.

2 PART A – AN INTRODUCTION TO DELINKING

2.1 Privacy and other fundamental rights in the EU

In the EU the right to privacy and data protection are considered fundamental rights. Article 6(1) of the TFEU recognises the rights, freedoms and principles set out in the Charter.⁷ Article 8(1) of the Charter states that “everyone has the right to the protection of personal data”, a right which is closely connected to the right to respect of “private and family life, home and communications” expressed in Article 7.⁸ Owing to this interrelationship, hereaf-

³ For example, through the use of ‘cookies’ or the retention of a person’s search requests.

⁴ European Commission, Directive 95/46/EC (23 November 1995) No. L281 *Official Journal of the European Union* 31-50.

⁵ *Google Spain SL & Anor v AEPD & Anor*, ECJ Case no. C-131/12, delivered 13 May 2014.

⁶ The version of the GDPR as passed by the European Parliament on 12 March 2014: *European Parliament legislative resolution of 12 March 2014 on the General Data Protection Regulation* (12 March 2014) (“EU Parliament Resolution”)

⁷ See Kuner, Christopher, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges* (15 September 2014), p2.

⁸ *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen*, ECJ Case No. C-92/09, delivered 9 November 2010 (“C-92/09”), [47].

ter the fundamental rights to data protection and privacy will simply be referred to as the right to privacy.

The right to privacy is not however an absolute right, and it is well established that it may be restrained by recognition of other fundamental rights. In this respect, two other fundamental rights are of particular relevance for present purposes. Article 11 of the Charter provides that everyone has the right to freedom of expression, including the right to receive and impart information and ideas without interference by public authority.⁹ Article 16 recognises the freedom to conduct business. The difficulty of reconciling these fundamental rights with one another in the case of a request for delinking is explored in Part C.

2.2 The idea of a right to erasure

In view of the ever increasing digital threat to privacy, there is a perceived need for greater online privacy protections for individuals. The right to erasure is one such form of protection. Conceptually, the idea is relatively simple; where appropriate, grant people the legal right to demand that an entity processing their data erase their personal information.

Notwithstanding the common reference to a right to be forgotten, as will be evident from the below discussion it is more appropriate to speak of the right as a right to erasure. This is because the right in its present form does not envisage broad notions of ‘forgetting’, but is simply concerned with a person’s right to demand erasure of their personal data held by others.¹⁰

⁹ See also, ECHR Article 10.

¹⁰ Cuijpers, Colette, Nadezhda Purtova and Eleni Kosta, *Data Protection Reform and the Internet: The Draft Data Protection Regulation* (Tilburg Law School Legal Studies Research Paper Series No.03/2014, Tilburg University, 2014), p10. McNealy, Jasmine, ‘The Emerging Conflict Between Newsworthiness and the Right to be Forgotten’ (2012) 39(2) *Northern Kentucky Law Review* 119, p121-122.

2.3 The right to delinking

2.3.1 How a search engine works

To begin with, it is appropriate to briefly introduce the manner in which a search engine actually operates. Given its dominant market role,¹¹ for present purposes it is adequate to focus on Google Search.

Google Inc, a US company, operates Google Search worldwide through the website google.com. Google Search begins by ‘crawling’ or searching webpages using software robots. Having discovered publicly available information, Google’s software organises that information into an index.¹² That index is currently “well over 100,000,000 gigabytes” and has taken over one million computing hours to build.¹³

When a user inputs a search query, Google’s algorithms look up the search terms in the index and display appropriate results. The exact manner in which the results are generated is not entirely known; the relevant algorithms are not publicly available, and accordingly some liken Google Search to a black box.¹⁴ However, Google does provide limited insight into the operation of its algorithms.¹⁵ Google’s algorithms rely on more than 200 unique signals or ‘clues’ that make it possible to guess what a user might be looking for. These signals include things like the terms on websites, the freshness of content, the user’s region and PageRank.¹⁶ While the algorithms operate automatically, they are obviously subject to human oversight and are continually updated. Also, on occasion Google manually edits its

¹¹ In 2013, it is estimated that Google held about 90 per cent of the global market share for internet search requests. The nearest competitors are Bing and Yahoo! with less than four per cent each; see Stuart, above n2, p472.

¹² See: Stuart, above n2, p473-474; *Google Spain*, [43].

¹³ Google, *Inside Search – How Search Works*.

¹⁴ Stuart, above n2, p472-473.

¹⁵ Google, above n13.

¹⁶ PageRank makes use of the link structure of the web to calculate a quality ranking for each webpage. It works by counting the number and quality of links to a webpage page, based on the assumption that more important websites are likely to receive more links: Brin, Sergey and Lawrence Page, ‘The anatomy of a large-scale hypertextual Web search engine’ (1998) 30 *Computer Networks and ISDN Systems* 107, p109-110. See also, Stuart, above n2, p474-475.

results; for example in the case of copyright, child sexual imagery or in order to remove spam.¹⁷

Google Search also incorporates a number of other features.¹⁸ For the purpose of this paper, it is sufficient to note that Google provides more relevant content based on geographic region. This includes providing, in some states, a locally adapted version such as google.no.

2.3.2 The different contexts in which delinking can be pursued

This paper will consider three different scenarios where a person might pursue delinking of search results. The first scenario is where a search request comprising the subject's name generates links to websites which are considered undesirable by the subject (hereafter called a "name-search"). The second scenario is where the search results to a particular search query (not specifically about the subject) include links to the subject in a manner that the subject considers undesirable (hereafter called a "non-name-search"). The third scenario sits between the first two; a search of the subject's name accompanied by a particular search query. For example, "Kim Kardashian Twitter Posts" (hereafter called a "composite-name-search").

It is important to note that in some cases where a subject has a right to delinking, that subject will also have a right to erasure against the actual website that is listed in the search results. In view of the preceding subsection, it follows that if that webpage itself is deleted then Google Search will no longer provide a link to that webpage in its search results.¹⁹ Accordingly, a right to erasure against a website can also indirectly lead to delinking from search results. The question which naturally follows is; why pursue the SEO and not the actual website?

¹⁷ Stuart, above n2, p475-476.

¹⁸ Google, above n13.

¹⁹ Alsenoy, above n2, p14.

2.3.3 Why pursue delinking from search engine results?

Broadly speaking, there are three main reasons why the right to delinking is attractive. The first reason stems from the indispensable role that search engines play in the operation of the internet. Search engines are the primary determinant of how most average internet users find information.²⁰ As one commentator noted:²¹

For finding information that is not otherwise presented to the user as an address or active link... Google is the Internet. Search engines are crucial, enabling Internet users' perusal of an otherwise-unmanageable number of websites.

Unsurprisingly, search engines are used extensively. For example, one study found that 73 per cent of all Americans use search engines.²² It follows that, for an internet user wishing to enforce their right to erasure, in many ways the SEO is the best place to start; delinking makes the information appreciably more difficult to find and thereby gives the subject a level of 'practical obscurity'.²³

The second reason delinking is attractive is because it is likely to be significantly easier than pursuing erasure against the actual websites. Given the ease at which online information can be replicated on other sites, a person may need to seek erasure from multiple different webpages in multiple jurisdictions.²⁴ In these circumstances enforcement against the websites is likely to be a time consuming, expensive and difficult process, to the extent that it may be an impractical option. By comparison the SEO, which acts as a gateway to the various websites, is likely to offer a user friendly means of lodging the delinking request.²⁵

²⁰ Stuart, above n2, p467-468, 471-472.

²¹ Stuart, above n2, p471. See also Alsenoy, above n2, p7.

²² Stuart, above n2, p471-472.

²³ Stuart, above n2, p470. *Google Spain*, [87].

²⁴ *Google Spain*, [84]. Alsenoy, above n2, p5.

²⁵ See, for example, the obligation in amended GDPR Article 19(2b).

Finally, delinking may achieve practical erasure in circumstances where the right to erasure is not legally enforceable against the website. This situation can arise in two ways; where the relevant website is hosted in a jurisdiction that does not recognise the right to erasure, or where the third party publication is lawful by reason of an exemption to the right.²⁶ In these situations, by proceeding against the SEO a person may be able to effectively enforce erasure even though they do not have a right against the actual website.

3 PART B – OVERVIEW OF THE EU RIGHT TO DELINKING

3.1 The DPD and the decision in *Google Spain*

3.1.1 The basis for the dispute in *Google Spain*

In 2010 Mr Gonzalez, a Spanish national resident, lodged a complaint with AEPD (the Spanish Data Protection Agency) against La Vanguardia (a Spanish Newspaper), Google Inc and Google Spain. The complaint arose from the fact that when an internet user did a name-search for Mr Gonzalez on google.es, the search engine generated links to two La Vanguardia news articles from early 1998. Those two articles contained an announcement of a real-estate auction connected with attachment proceedings against Mr Gonzalez for the recovery of social security debts.²⁷

In his complaint, Mr Gonzalez requested that La Vanguardia remove or alter the webpages. He also requested that Google Spain or Google Inc be required to remove or conceal the links in the search results. As the attachment proceedings were resolved many years earlier, Mr Gonzalez argued the references were irrelevant.²⁸

²⁶ *Google Spain*, [85]-[86].

²⁷ *Google Spain*, [14]. Advocate General Jääskinen, *Opinion of Advocate General Jääskinen delivered 25 June 2013 – Case C-131/12 – Google Spain SL & Anor v AEPD & Anor* (25 June 2013) (“AG Opinion”), [18].

²⁸ *Google Spain*, [15].

3.1.2 Procedural history

The AEPD rejected the claims against La Vanguardia on the basis that its publication was legally justified.²⁹ However, the AEPD upheld the complaint against Google Spain and Google Inc.

Google Spain and Google Inc subsequently commenced actions in the Audiencia Nacional (National High Court) against the decision by AEPD.³⁰ The Spanish Court referred a number of questions concerning the DPD to the ECJ for a preliminary ruling.³¹ Essentially, those questions can be broadly summarised as concerning the following three issues: the ‘territorial scope’ of the DPD;³² whether Google Inc, in providing Google Search, was ‘processing’ data and a ‘controller’;³³ the scope of a data subject’s rights under DPD Articles 12(b) and 14(a), and whether there is a right to require delinking from the results in a name-search.³⁴

3.1.3 Judgment – first issue – the ‘territorial scope’

As to the relationship between Google Inc and Google Spain, it was established that Google Inc was responsible for Google Search, including google.es, and that it conducted those activities outside of the EU. The activities of Google Spain were limited to promoting the sale of advertising space and acting as the commercial agent for Google Inc.³⁵ Accordingly, only Google Inc dealt directly with personal data with respect to Google Search.

²⁹ Ibid, [16].

³⁰ Ibid, [18].

³¹ AG Opinion, above n27, [6].

³² *Google Spain*, [45].

³³ Ibid, [21].

³⁴ It is acknowledged that the ECJ drew a distinction between referred Questions 2(c) and 2(d), and Question 3; see, respectively, [62]-[88] compared to [89]-[99]. However, on a proper analysis this author considers there is no meaningful distinction between the two questions; both essentially concerned the scope of the right to erasure and the Court offered analogous reasoning in each case. Accordingly, the two questions will be dealt with together.

³⁵ *Google Spain*, [43], [46], [51].

DPD Article 4(1)(a) provides that Member States must apply their national laws to processing carried out in the context of the activities of an establishment of the controller in the Member State. Given the relationship between Google Inc and Google Spain, the ECJ concluded that the processing of personal data by Google Inc occurred in the context of Google Spain's commercial and advertising activities in Spain (the activities of the two entities were inextricably linked).³⁶ Accordingly, the DPD applied to the activities of Google Inc in providing its Google Search function in Spain.

3.1.4 Judgment – second issue – ‘processing’ and ‘controller’

This question concerned whether Google Inc, in providing Google Search, was “processing personal data” and a “controller” of that data. Under Article 2(1)(b), “processing of personal data” is defined as any operations performed upon personal data, whether or not by automatic means, such as (inter alia) collection, recording, organisation, storage, retrieval or making available. The ECJ noted that Google Inc, in providing Google Search, searches the internet for published information, ‘collects’ such data and subsequently ‘retrieves’, ‘records’ and ‘organises’ it as part of its indexing programmes. Therefore, the ECJ held that in view of the wording in Article 2(1)(b) such activity clearly constituted processing.³⁷

“Controller” is defined in Article 2(1)(d) of the DPD as the natural or legal person which alone or jointly with others determines the purposes and means of the processing. Google Inc argued it was not a controller since it had no knowledge of the data and did not exercise control over it (that control inherently being with the website publisher).³⁸ However, the ECJ had little difficulty concluding that a SEO is a controller. Reciting the definition of controller, it held that a SEO clearly determines the “purposes and means” of the processing. It was noted that this processing can be distinguished from, and is additional to, processing carried out by the actual webpage publisher. Therefore, it did not matter that the

³⁶ Ibid, [56].

³⁷ Ibid, [28].

³⁸ Ibid, [22].

search engine does not exercise control over the actual publication of the data on the internet.³⁹

3.1.5 Judgment – third issue – the scope of the right to delinking

The third issue essentially concerned whether a subject could require delinking from the results of a name-search based on Articles 12(b) and 14(a) of the DPD. Article 12(b) provides that a data subject has the right to obtain from a controller the “rectification, erasure or blocking” of data where that processing does not comply with the Directive. Per Articles 6(1)(c) to (e), the processing may not comply if it is inadequate, excessive or no longer relevant, or excessive in relation to the purpose of the SEO’s processing.⁴⁰

The SEO’s processing may also not comply with the Directive if Article 7(f) is not met. Under that Article, the processing by a SEO is lawful because it is necessary for the legitimate interests of the SEO.⁴¹ However, Article 7(f) requires that the SEO’s legitimate interests not be overridden by the fundamental rights of the subject. Therefore, the application of Article 7(f) necessitates a balancing of opposing rights and interests.⁴² If the subject’s rights do override the legitimate interests of the SEO, there are two potential implications. Firstly, the processing does not comply with the Directive and Article 12(b) is enlivened.⁴³ Secondly, if a subject has objected to the processing on “compelling legitimate grounds” under Article 14(a), that objection would be justified and per Article 14(a) the data may no longer be processed by the SEO.⁴⁴

The ECJ proceeded on the basis that applying Articles 12(b) and 14(a) essentially required a balancing of the data subject’s right to privacy against the legitimate economic interests of the SEO and the interests of internet users in accessing the information. The ECJ considered that a name-search is liable to significantly affect the subject’s privacy since it enables

³⁹ Ibid, [32]-[40].

⁴⁰ Ibid, [93]-[94].

⁴¹ Ibid, [73]-[74]. See also AG Opinion, above n27, [95].

⁴² *Google Spain*, [74].

⁴³ Ibid, [75], [95].

⁴⁴ Ibid, [76], [95].

a “more or less detailed profile” to be established with relative ease.⁴⁵ Given the seriousness of this interference, the ECJ was of the view that it could not be justified merely by the economic interests of the SEO. As to the interests of internet users in accessing information, the ECJ considered that as a general rule those rights were overridden by the data subject’s right to privacy. However, the ECJ acknowledged that this balancing would ultimately depend on the nature of the information in question, the sensitivity of the information, the subject’s role in public life and the public interest in the information.⁴⁶ The Court concluded that, subject to the appraisal favouring delinking, a SEO is obligated to remove the relevant results from a name-search even when the publication is lawful and the data will remain on the internet.⁴⁷

3.1.6 Summary of the position under the DPD

In *Google Spain*, the ECJ recognised in principle that under the DPD a person has a right to require delinking from the results of a name-search when the conditions in Articles 12(b) or 14(a) are met. The Court held that while the existence of this right requires a balancing of the conflicting fundamental rights, as a “general rule” the subject’s right to privacy should prevail.

However, the judgment left a number of issues unanswered. In particular, there is considerable uncertainty as to how a SEO is to appropriately assess a request for delinking if it is not factually analogous to *Google Spain*. While this issue is explored in Part C, before undertaking that discussion the next subsection introduces the new proposed data regulation, the GDPR.

3.2 The GDPR

In January 2012 the European Commission proposed reform of the DPD. The proposal consisted of a draft Regulation setting out a general EU framework for data protection (the

⁴⁵ Ibid, [80].

⁴⁶ Ibid, [81].

⁴⁷ Ibid, [82].

GDPR), and a draft Directive concerning personal data processing for criminal offences and related judicial activities.⁴⁸ It is the GDPR, which contains provisions concerning the right to erasure, which is relevant to this paper.

The GDPR is in the form of a regulation and does not require transposition;⁴⁹ following a two year transition period after its adoption the regulation has binding legal force within each Member State.⁵⁰ The original Commission proposal was finalised on 25 January 2012.⁵¹ On 12 March 2014, the European Parliament voted in favour of a slightly amended version of that proposal.⁵² The next step is for the amended GDPR to be considered by the Council.⁵³ As of November 2014, the Council has not voted on the proposal.

This subsection will examine whether the GDPR in its current form provides a right to de-linking, and if it does whether, prima facie, that right is likely to operate in a similar manner to the current position under the DPD. Given the uncertainty involved in the legislative process, it would be a fool's exercise to try and predict with any specificity the final form of the instrument. Indeed, given recent amendments by the European Parliament the GDPR version currently before the Council is in some aspects materially different from the original Commission proposal. Unfortunately, brevity precludes a detailed analysis of both versions. That being so, as a pragmatic solution this paper will focus on the version approved by Parliament on 12 March 2014 since this is the most recent incarnation. However, where

⁴⁸ European Commission, *Memo/14/60 – Data Protection Day: Full Speed on EU Data Protection Reform* (European Commission Memo, European Commission Strasbourg, 27 January 2014) (“Memo/14/60”).

⁴⁹ European Commission, *Application of EU law – What are EU Regulations?* (25 June 2012). Shoor, Emily, ‘Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation’ (2014) 39(1) *Brooklyn Journal of International Law* 487, 2014, p490. European Commission, *General Data Protection Regulation*, (Brussels, 25 January 2012) (“Original GDPR”).

⁵⁰ GDPR, above n6, Article 91(2).

⁵¹ European Commission, *Press release - Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* (25 January 2012).

⁵² European Parliament, *Press Release – MEPs tighten up rules to protect personal data in the digital era* (12 March 2014) (“EU Parliament Press Release”).

⁵³ European Commission, *Memo/14/186 - Progress on EU data protection reform now irreversible following European Parliament vote* (European Commission Memo, European Commission Strasbourg, 12 March 2014). Memo/14/60, above n48.

it is instructive to the analysis of this amended version limited regard will be had to the original Commission proposal and the reasons for its amendment by Parliament.

3.2.1 Outline of Article 17 – a right to erasure

Article 17 is a relatively lengthy provision. For present purposes, the following outline is sufficient. Amended Article 17(1) provides that:⁵⁴

The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, and to obtain from third parties the erasure of any links to, or copy or replication of, that data where one of the following grounds applies...

The relevant grounds are: per 17(1)(a), the data is no longer necessary; per 17(1)(b), absent some other justification, the data subject withdraws their consent; per 17(1)(c), the subject objects on the grounds of amended Article 19; per 17(1)(ca), a court or regulatory authority has ordered the erasure; per 17(1)(d), the data has been processed unlawfully.

Amended Article 17(3)(a) requires that the controller, and where applicable third parties, carry out erasure without delay unless retention is necessary for exercising the right of freedom of expression in accordance with Article 80. The exemptions under Article 80 are to be provided for by each Member State.⁵⁵

3.2.2 Article 17 and search engine results

3.2.2.1 “Controller” and “third parties”

The first issue is whether a SEO is considered a controller under the GDPR and Article 17(1). The definition of “controller” in the GDPR does not differ materially in any way

⁵⁴ EU Parliament Resolution, above n6, Amendment 112.

⁵⁵ With each Member State to notify the Commission of their provisions within two years: see European Parliament Resolution, above n6, Amendments 112, 189, Articles 80(2), 91(2).

from the DPD.⁵⁶ Likewise, the GDPR does not contain any distinguishing recitals with respect to the definition. Accordingly, it can be logically reasoned that based on *Google Spain* a SEO is likely to be considered a controller under the GDPR.

However, because of the reference in amended GDPR Article 17(1) to “third parties”, as opposed to the DPD the existence of a right to delinking in the GDPR is not dependant on the SEO being considered a controller. And, in view of the definition in amended GDPR Article 4(7a),⁵⁷ it is certainly possible for a SEO be considered a “third party”.

It is interesting in this respect that the European Parliament considered it necessary to amend the original proposal (which did not contemplate erasure from third parties). It is possible that the amendment was included in specific contemplation of SEOs as third parties as opposed to controllers, although the rationale for the amendment is unclear. For reasons that will be explored in Part C, there are strong arguments favouring an interpretation of SEOs as third parties.

In any event, irrespective of whether SEOs are considered controllers or third parties it follows that Article 17 appears to contemplate SEOs within its scope. Indeed, in a recent public session of the Justice and Home Affairs Council which specifically considered Article 17 in light of *Google Spain* (hereafter referred to as the “JHAC Public Session”), the overwhelming majority of representatives appeared content with the concept of a right to delinking under the GDPR.⁵⁸

3.2.2.2 Objection under Article 17(1)(c)

Given this conclusion that SEOs will come within the scope of amended GDPR Article 17(1), the next question is whether the subject has a requisite ground under Article 17(1) on which to object. With respect to the right to delinking, the relevant ground for objection is

⁵⁶ See EU Parliament Resolution, above n6, amended Article 4(1)(5), and DPD Article 2(d).

⁵⁷ EU Parliament Resolution, above n6, Amendment 98.

⁵⁸ Council of the European Union, *Justice and Home Affairs Council – Public Session, Friday, October 10, 2014 at 10:10am* (Webcast, 10 October 2014) (“JHAC Public Session”), from 51:00 onwards.

contained in Article 17(1)(c). This Article gives the subject the right to object to the processing on the grounds of amended Article 19.

Amended Article 19 operates as follows.⁵⁹ Under GDPR Article 6(1)(f), processing by a controller is lawful when it “is necessary for the purposes of the legitimate interests pursued by the controller... except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject”. Applying *Google Spain*, Article 6(1)(f) provides the relevant legitimisation for processing by a SEO.⁶⁰ Where a controller’s processing is based on Article 6(1)(f), amended Article 19(2) provides that “the data subject shall have at any time and without any further justification, the right to object free of charge in general or for any particular purpose...”. Therefore, Article 17(1)(c) read in conjunction with Article 19 gives a subject an unqualified right to object with respect to processing by a SEO.

3.2.2.3 Exemption under Article 17(3)(a)

Article 17(3) provides that a SEO, faced with an objection based on Article 17(1)(c), must carry out erasure without delay unless retention is necessary for one of several enumerated reasons. In the case of a request for delinking, the most relevant exception⁶¹ is contained in Article 17(3)(a).

Article 17(3)(a), read in conjunction with amended Article 80, provides an exemption where retention of the data is necessary for exercising the right of freedom of expression in accordance with the Charter.⁶² Amended Article 80 broadens the language from the original Commission proposal. The original language, which was analogous to that used in the

⁵⁹ EU Parliament Resolution, above n6, Amendment 114.

⁶⁰ Article 6(1)(f) is analogous to the DPD ‘legitimate interest’ provision contained in Article 7(f); see *Google Spain*, [73]-[74].

⁶¹ However, it is acknowledged that *in certain circumstances* the exemption in Article 17(3)(b) concerning public health, or 17(3)(c) concerning “historical, statistical and scientific research purposes”, could also be relevant.

⁶² EU Parliament Resolution, above n6, Amendments 112, 189.

DPD,⁶³ only mandated an exemption for processing “carried out solely for journalistic purposes or the purpose of artistic or literary expression”. The European Parliament also broadened the accompanying Recital 121 in the same manner. The first part of the amended Recital 121 now provides:⁶⁴

Whenever necessary, exemptions or derogations from the requirements of certain provisions of this Regulation for the processing of personal data should be provided for in order to reconcile the right to the protection of personal data with the right to freedom of expression, and notably the right to receive and impart information...

In amending the original version and adopting this language, the European Parliament’s version appears to stress the importance of reconciling the right to privacy with all forms of freedom of expression (that is, not just in the case of journalistic, literary or artistic expression). Therefore, arguably the amended GDPR contemplates greater deference being given to the right to freedom of expression. This interpretation accords with views expressed in the recent JHAC Public Session.⁶⁵ In that session, several representatives expressed concern that *Google Spain* appeared to grant primacy to the right to privacy, with inadequate consideration of the equally important conflicting fundamental rights.

The second part of amended Recital 121 is also relevant. It provides that:⁶⁶

In order to take account of the importance of the right to freedom of expression in every democratic society, it is necessary to interpret notions relating to that freedom broadly to cover all activities which aim at the disclosure to the public of information, opinions or ideas, irrespective of the medium which is used to transmit them... They should not be limited to media undertakings and may be undertaken for profit-making or for non-profit making purposes.

⁶³ See DPD Article 9.

⁶⁴ EU Parliament Resolution, above n6, Amendment 83 (emphasis added).

⁶⁵ JHAC Public Session, above n58. See, for example, webcast around 52:20 (Luxembourg), 56:00 (France), 1:00:00 (Germany), 1:04:00 (Poland), 1:26:00 (Estonia).

⁶⁶ Emphasis added.

Given the vital role of SEOs in disseminating information, potentially this recital provides increased scope for exempting their processing from the right to erasure. It could be argued that, based on the reference to “all activities which aim at the disclosure” “irrespective of medium”, if the processing by the website is justified so too is the processing by the SEO as an activity aimed at disclosing that information.

However, it must be remembered that in *Google Spain* the ECJ drew a sharp distinction between the processing by La Vanguardia and the processing by Google. The Court reasoned that as there were two distinct forms of processing, the lawfulness of the former did not necessarily mean the latter was also lawful.⁶⁷ Under this compartmentalised approach, whereby the conduct of the website and SEO are considered in relative isolation, notwithstanding the wording in Recital 121 there is limited scope for drawing a nexus between the lawfulness of the website publishing and the processing by the SEO.

It must also be acknowledged that the GDPR appears to essentially contemplate a balancing of the competing rights in a manner not dissimilar to that undertaken in *Google Spain*. Indeed, following the decision the European Commission stated that GDPR Article 80 “...specifically asks for the type of balancing that the Court outlined in its ruling.”⁶⁸ In this respect, it is relevant to recall that in conducting this balance under the DPD the ECJ had little difficulty concluding that the data subject’s rights “override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information”.⁶⁹

In these circumstances it appears reasonable to submit that, prima facie, a materially different approach to delinking under the GDPR does not seem likely. However, the complexity of how the right might actually operate under the GDPR will be more fully explored in Part C.

⁶⁷ *Google Spain*, [85], [87].

⁶⁸ European Commission, *Factsheet on the “Right to be Forgotten ruling” (C-131/12)*. See also statements by the Commission representative at the JHAC Public Session, above n58, at 49:30, to the effect that the ruling in *Google Spain* confirms the balancing of rights on which the entire GDPR proposal is based.

⁶⁹ *Google Spain*, [97].

3.2.2.4 Third party notification and Article 17(2)

Amended Article 17(2) provides that where a controller has made the data “public without a justification based on Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties”.⁷⁰ Under this amended Article, it appears the notification obligation is tied to the culpability of the controller who made the data public in the first place.⁷¹ As discussed above, the lawfulness of processing by a SEO arises under GDPR Article 6(1)(f). Therefore, it appears the notification obligation should not attach to SEOs.⁷²

3.2.3 Summary of the right to delinking under the GDPR

It is impossible to predict what form Article 17 will ultimately take. However, and having established this caveat, it is acknowledged that Article 17 clearly has the support of the European Commission who drafted it. Further, the European Parliament approved the GDPR by an overwhelming majority of 621 votes to 10, with only minor amendments to Article 17.⁷³ And, in the recent JHAC Public Session, the overwhelming majority of Council representatives appeared in favour of a right to delinking.⁷⁴ In these circumstances, it appears a right to require delinking will exist under the GDPR.

⁷⁰ In the original version of the GDPR, Recital 54 and Article 17(2) contemplated an obligation on all controllers to take “reasonable steps, including technical measures” to inform third parties processing the data that the subject had requested erasure: see Original GDPR, above n49. This obligation was poorly considered, since it would have been almost impossible for a SEO to comply with it; it would be impractical for the SEO to inform every party that had conducted the name-search about the delinking request.

⁷¹ The correct interpretation appears to be that the obligation in Article 17(2) is tied to the lawfulness of the original public disclosure. Accordingly, the requisite finding of unlawfulness at the time of the data subject’s objection (which *may* grant the right to erasure), does not apparently enliven Article 17(2). Otherwise the reference to “without a justification” in Article 17(2) would be superfluous and nonsensical. See also, Albrecht, Jan Philipp, *Report A7-0402/2013* (21 November 2013), p201, 300-301.

⁷² However, the wording of amended Article 13 is still potentially problematic. It would be appropriate to clarify that SEOs do not “transfer” data in providing their search function, although by amending the original wording from “disclose” to “transfer” it appears a higher threshold is contemplated. See EU Parliament Resolution, above n6, Amendment 108.

⁷³ EU Parliament Press Release, above n52.

⁷⁴ Albeit, while stressing the importance of balancing competing rights: JHAC Public Session, above n65. However, notably the representative for Britain was critical of *Google Spain*, remarking that it was “Open to us, as legislators, to reach a different conclusion”: around 1:16.00..

4 PART C – A CRITICAL ANALYSIS OF THE RIGHT TO DELINKING

This section will provide a critical analysis of the right to require delinking from search engine results. In view of the discussion in Part B, it is submitted that conceptually the right to delinking under the DPD and GDPR are not materially different. Accordingly, the below discussion will for the most part proceed without distinction between the two instruments.

Part C is structured as follows. The discussion will begin by setting out the criteria against which the right to delinking will be assessed. With this providing the appropriate basis for a critical analysis, the discussion will in turn look at the following four issues: the manner in which the framework balances the various conflicting fundamental rights; whether it is appropriate for a SEO to be considered a “controller”; the extra-territorial operation of the right; and the potential economic implications.

4.1 Criteria for assessment – privacy, freedom of expression and intermediary liability

In order to critically examine the right to delinking, it is first necessary to outline the basis against which it will be assessed. The right to delinking, as set out above, is merely one facet of the broader right to erasure. At its core, it is reasonable to submit that the right to erasure is concerned with privacy protection. However, the very notion of ‘privacy’ is inherently difficult to define,⁷⁵ and it has been said that “data privacy law has long been afflicted by absence of clarity over its aims and conceptual foundation”.⁷⁶ While a comprehensive examination of the rationale for privacy protection is clearly beyond the present scope, in short safeguarding privacy serves a range of interests such as personal autonomy,

⁷⁵ Bygrave, Lee, *Data Privacy Law – An International Perspective* (Oxford University Press, 2014), p119.

⁷⁶ *Ibid*, p117.

integrity and dignity, which in turn have broader societal significance.⁷⁷ And, as already set out in Part A, the right to privacy is considered a fundamental right in the EU.

At the same time, as set out in Part A the freedom of expression, to which the right to receive and impart information are integral, and the freedom to conduct business, are fundamental rights in the EU. While brevity precludes a full analysis, these rights are undeniably of central importance. For example, freedom of expression is essential to a functioning democracy, and indispensable for progress in science, law or politics. The freedom to conduct business is essential to the free-market ideas that underpin our modern economic model.

As is clear from Parts A and B, generally the right to delinking cannot be recognised without interfering with the fundamental rights of others. Therefore, the competing fundamental rights must be appropriately reconciled with one another. The problem is that, in resolving this conflict, there is no formal hierarchy between the fundamental rights and there is no objectively infeasible correct outcome; the world of rights is two-dimensional, and they all lie on the same straight line.⁷⁸ As the representative for France recently stated at the JHAC Public Session, “we have to reconcile two things which are rather irreconcilable”.⁷⁹ It follows that an assessment of where the appropriate balance lies is inherently coloured by what one considers to be the desired outcome, and the trade-offs that one is willing to make to reach that outcome. This assessment is, therefore, innately subjective in nature.

That being the case, it is perhaps not surprising that views on the right to erasure vary dramatically. On the one hand, the right can be seen as a valuable tool to temper the modern “flawless digital memory”.⁸⁰ In this sense, recognition of the right is justified because it is a socially beneficial means to facilitate individuals reforming their lives without the continu-

⁷⁷ Ibid, p119-120.

⁷⁸ House of Lords European Union Committee, *EU Data Protection law: a ‘right to be forgotten’? Evidence* (July 2014), Professor Luciano Floridi, p19.

⁷⁹ JHAC Public Session, above n58, around 55:00 onwards.

⁸⁰ Kulevska, Sanna, *Humanizing the Digital Age: A Right to be Forgotten Online? – An EU-U.S. Comparative Study of Tomorrow’s Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD* (LLM Graduate Thesis, Lund University, May 2014), p1.

ous burden of their past mistakes.⁸¹ On the other hand the right to erasure, as a right which limits society's access to truthful, valuable, publicly available information, is so repugnant to freedom of expression that its existence should not be recognised. To some this discourse has particular authority in the context of the internet, since the internet is an immensely important, widely accessible, non-discriminatory resource which magnifies and facilitates in an unprecedented manner the efficient dissemination of valuable information.⁸²

In the context of the internet, a further complication arises in this debate in the form of intermediary liability. Since many internet intermediaries do not actively control the content they store, transmit or make accessible, and in view of the large quantities of information with which they deal, there is an established notion that such intermediaries should not face the same level of responsibility as traditional publishers. Otherwise, the expansion of the internet and freedom of expression would be improperly threatened.⁸³ This principle is recognised in the EU,⁸⁴ although opinions differ as to how the activities of SEOs fit within the concept of internet intermediaries.⁸⁵ Given the present scope, a full analysis is inappropriate. The limited point to take away is that, broadly speaking, the very concept of regulating SEOs involves complex questions concerning the regulation of online intermediaries.

The purpose of the above (albeit superficial) discussion is to highlight that at its heart any assessment of the right to erasure is intrinsically complex, involving broad fundamental value judgements about how the right to privacy, freedom of expression and freedom of business should be legally balanced; a discussion which is, in itself, a topic of academic scholarship and entirely inappropriate in view of the present scope. Therefore, caution must

⁸¹ Baker, Michael and Alan Westin, *Databanks in a Free Society; Computers, Record-Keeping, and Privacy* (1972, Quadrangle Books), p267. Kulevska, above n80, p7. Peltz-Steele, Richard, 'Right to be forgotten' is effectively a right to be forgiven, *The Sydney Morning Herald* (Online) 24 November 2014.

⁸² See generally: AG Opinion, above n27, [28]. Alsenoy, above n2, p5.

⁸³ Alsenoy, above n2, p58.

⁸⁴ See, for example, European Commission, 'Directive 2000/31/EC' (17 July 2000) No. 178 *Official Journal of the European Union* 1-16. See also, Alsenoy, above n2, p58-63.

⁸⁵ Alsenoy, above n2, p63.

be exercised to avoid becoming improperly entangled in analysis of such a fundamental tension.

Therefore, for present purposes this paper will adopt the following pragmatic approach. It will be accepted that SEOs pose a serious threat to the right to privacy, but it will equally be accepted that SEOs are potentially champions of the right to freedom of expression.⁸⁶ That being so, the discussion will not seek to argue in principle that the right to delinking is inherently repugnant or inherently desirable. Rather, the present critical analysis will focus on the manner in which the right *actually operates*. As such, the analysis will concentrate on the extent to which the right provides an acceptable framework for balancing the conflicting fundamental rights, and can be applied in a practical, equitable, efficient and certain manner.

4.2 Balancing the competing interests

As outlined above, under both the DPD and GDPR the existence of a right to delinking essentially requires that the SEO balance the subject's right to privacy against the conflicting fundamental rights of the other affected parties. There are two main problems that arise from this operation; how to strike the appropriate balance, and whether it is appropriate for a SEO to make this decision. This subsection will consider these two issues in turn.

4.2.1 Google on a tightrope

As introduced in Part B, the DPD and GDPR differ as to the mechanics of how the right to delinking actually operates. As such, given the focus of this subsection it is appropriate to discuss each instrument separately.

4.2.1.1 The DPD

This section will examine, in turn, the following three issues arising under the DPD: whether the ECJ in *Google Spain* inappropriately gave primacy to the right to privacy;

⁸⁶ Alsenoy, above n2, p5.

whether the DPD, in view of *Google Spain*, provides an adequate framework for SEOs to assess delinking requests; how the right to delinking might operate with respect to non-name-searches.

4.2.1.1.1 *Google Spain – a knock out for privacy?*

The focus of this subsection is whether the ECJ in *Google Spain* demonstrated an inappropriate preference for privacy protection over other fundamental rights. However, before turning to the specific concerns about the judgment it is necessary to explore in more detail how the right to delinking impacts on the rights of the various parties.

With respect to the data subject, their right to privacy is protected by the right because without it a name-search may allow any internet user to obtain “a more or less detailed profile” of them with relative ease.⁸⁷ On the other hand, delinking may interfere with the rights to freedom of expression and business enjoyed by SEOs, internet users and website publishers. For a SEO, their activity of providing the search function and selling advertising are in principle protected by their right to freedom of expression and business.⁸⁸ For internet users, search engines facilitate the retrieval of information. When a user enters a name-search, they are actively exercising their right to find information about that subject. If the search results are altered, that user’s right is interfered with.⁸⁹ For website publishers, their right to freedom of expression and business generally protects their right to publish lawful content and have that content disseminated by SEOs. If links to their webpages are removed from search results, their rights are interfered with.⁹⁰

⁸⁷ *Google Spain*, [80].

⁸⁸ There is a line of argument that in publishing search results SEOs are exercising their right to expression, and therefore deserve the relevant protection. See: Alsenoy, above n2, p50-51; AG Opinion, above n27, [132]. This argument has found favour in the US as a means for SEOs to obtain protection from liability under the first amendment. See, Stuart, above n2, p487-490.

⁸⁹ Alsenoy, above n2, p50. AG Opinion, above n27, [121], [130]-[131].

⁹⁰ AG Opinion, above n27, [122].

In striving to protect privacy by establishing the right to delinking, it must be examined whether the right to delinking is relevant, efficient and proportionate⁹¹ to the legitimate privacy aims pursued.⁹² The concern is that, based on the approach in *Google Spain*, the right to delinking might operate in a way that does not respect these criteria, and does not therefore strike an appropriate balance between the conflicting fundamental rights. In this respect, the apprehension arises because arguably the ECJ demonstrated an inappropriate preference for protecting the right to privacy without proper consideration of the competing rights; a concern which was recently raised by a number of representatives at the JHAC Public Session.⁹³ This subsection will examine four particular aspects of the Court's decision which are potentially troubling.

The first area of concern arises from the Court's statement that, given the "potential seriousness" of the interference with privacy caused by a name-search, "it is clear that it cannot be justified merely by the economic interest" of the SEO.⁹⁴ The issue here is why the mere *potential* for a serious interference is sufficient. In providing its search function the SEO is exercising its fundamental rights to both freedom of expression and business.⁹⁵ As set out above, in reconciling these rights against the subject's right to privacy there is no formal hierarchy, and the appropriate balance should be struck on a case-by-case basis.⁹⁶ Therefore, *prima facie* it appears inappropriate for the ECJ to de facto subrogate the SEO's fundamental rights. Adherence to the principle of proportionality should require consideration of whether, on the facts, there is an actual serious interference or risk of a serious interference. Indeed, depending on the relevant facts this may not always be the case.⁹⁷

⁹¹ The principle of proportionality is generally considered to have three limbs; suitability, necessity and non-excessiveness. See Bygrave, above n75, p148.

⁹² *Österreichischer Rundfunk v. Austria*, ECtHR Case no. 35841/02, 7 December 2006, [62]. See also, Alsenoy, above n2, p70.

⁹³ JHAC Public Session, above n65.

⁹⁴ *Google Spain*, [81].

⁹⁵ AG Opinion, above n27, [132]. Alsenoy, above n2, p57.

⁹⁶ Alsenoy, above n2, p66.

⁹⁷ For example, and discussed in the next subsection, where the data subject has a particularly common name.

The second area of concern arises from the Court’s statement that “as a general rule” the rights of the data subject override those of the internet user. Arguably, the reference to a “general rule” is inappropriate (even though it was qualified by the Court).⁹⁸ Again, as there is no hierarchy between the competing rights it does not seem appropriate to assume the balance lies in favour of the data subject; the conflicting rights should be reconciled depending on the facts of the case.⁹⁹

In considering the rights of the internet user, it is important to remember that their right to freedom of expression includes the right to receive information. As the AG commented, when an internet user performs a name-search that user “is *actively using his right to receive information concerning the data subject from public sources* for reasons known only to him”.¹⁰⁰ The AG continued by noting that, in the contemporary information society, performing a search online is “one of the most important ways to exercise that fundamental right”.¹⁰¹ In this author’s opinion, the AG’s comments hold particular significance. An internet user performing a name-search is actively exercising their right to find publicly available information about that person, for reasons which might be entirely legitimate and extremely important to that user. To the extent those search results are compromised by delinking, this might potentially constitute a serious interference with that user’s right to receive the information they are searching for. That being so, it seems entirely improper for the ECJ to succinctly conclude that given the “potential seriousness” of the interference to the data subject, the subject’s rights “as a general rule” override those of the internet user. Such a presumption represents an unjustified value judgment that the potential interference with the data subject is more serious than the potential interference with the internet user. Rather, the determination should depend on the facts of the particular case, and it is inappropriate to commence such analysis with a presumption in favour of one party.

⁹⁸ *Google Spain*, [81], and see also at [97], [99].

⁹⁹ However, it is acknowledged that the matter was ultimately left for the referring court, albeit with the ECJ providing its view that “in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that information...”: *Google Spain*, [98].

¹⁰⁰ AG Opinion, above n27, [130] (emphasis original).

¹⁰¹ *Ibid*, [131].

The third area of concern relates to the ECJ's statement that the existence of the right to delinking does not require a finding that the relevant search results cause prejudice to the data subject.¹⁰² Whether this comment is controversial depends upon its intended meaning. If the Court merely intended to establish that a factual finding of prejudice is not a criterion for applying the right, the statement is inoffensive; it is well-established that protection of privacy, as a fundamental right, is not conditional on prejudice. However, it is also possible to interpret the Court's comments as suggesting that the privacy interests of the data subject are to be favoured. This is because, in balancing the competing interests, the restrictions on freedom of expression must be relevant and proportionate to the legitimate privacy aims pursued by the subject; an analysis that demands consideration of the subjective privacy implications for the subject. Therefore, in short *it is relevant* to the requisite balancing whether the subject suffers prejudice. Ultimately, the judgment is unclear as to which interpretation was intended by the Court. Since the Court gave specific consideration at paragraph 98 to the impact on Mr Gonzalez from the "sensitive" La Vanguardia articles, it can be reasoned that the former interpretation was intended. However, arguably it would have been beneficial for the Court to clarify that prejudice to the data subject, while not strictly required, should be taken into account in balancing the relevant interests.

The fourth issue with the approach taken by the ECJ arises from the Court's failure to acknowledge the website publisher's right to freedom of expression and business.¹⁰³ When a person lawfully publishes an article online about a data-subject, that person is actively invoking their right to disseminate information about that subject. In the modern age, one aspect of this right is the potential to have the article included in the results of a name-

¹⁰² *Google Spain*, [96], [99].

¹⁰³ On a strict interpretation of the DPD there is some uncertainty as to whether the Court was required to take the publishers' interests into account. Under DPD Article 7(f) regard is to be had to the legitimate interests of the SEO (controller) and parties to who the data are disclosed (internet users). Accordingly the assessment does not, strictly speaking, contemplate that the impact on the fundamental rights of other parties (in this case publishers) be taken into account. However, it can be reasonably argued that based on the principle of proportionality these interests should be taken into consideration. As to proportionality, see *Bodil Lindqvist*, ECJ Case no. C-101/01, [89]. Indeed, the AG's opinion included consideration of the interests of the website publishers; see AG Opinion, above n27, [122].

search about the subject.¹⁰⁴ While the rights of the publisher may be overridden by the privacy rights of the subject, those conflicting rights must actually be balanced. In the circumstances of *Google Spain*, this exercise would not likely have had material affect; given the relevant newspaper articles concerned announcements of a property sale 16 years ago, it would not be controversial to find that La Vanguardia’s right to have those articles disseminated in the name-search were overridden by the privacy interests of Mr Gonzalez. However, arguably it was inappropriate that the Court failed to acknowledge that, depending on the facts of the case, consideration should be given to the publisher’s rights. Indeed, in certain circumstances the rights of the publisher may strongly mitigate against delinking.¹⁰⁵

In view of the above, it can be reasonably argued that the approach adopted by the ECJ in *Google Spain* was in some respects less than ideal. While the Court did not necessarily reach the wrong conclusion on the facts,¹⁰⁶ the method it adopted suggests an inappropriate preference for the rights of the data subject. Contrary to the impression given by the Court, the various conflicting rights should be treated equally, with a determination made on the facts of the case. The next section explores the difficulties that arise for SEOs in applying this framework.

4.2.1.1.2 *Applying the current framework*

It has been a common theme of this paper that the application of the right to delinking essentially turns on a balancing of the various fundamental rights involved. The difficulty of reconciling these conflicting rights is itself a scholarly topic, and one to which this subsection will not attempt to make a comprehensive addition. Rather, the present discussion will merely examine some specific difficulties that arise in assessing a delinking request.

In view of the preceding subsection, for a SEO assessing a delinking request there is a degree of uncertainty as to whether it is entitled to proceed on the basis of the “general rule”

¹⁰⁴ Assuming the publisher has not made use of an exclusion code. See AG Opinion, above n27, [41], [122].

¹⁰⁵ An issue which is explored in the next subsection.

¹⁰⁶ Although that may certainly be the opinion of some, perhaps most notably the AG.

in favour of the data subject, or whether the assessment demands an individual examination of the particular facts. In this respect, this paper submits that the precedential effect of *Google Spain* should be limited to the facts in which it was decided, namely an application by a non-public figure about prejudicial, outdated and reasonably irrelevant information. For delinking requests in an analogous factual context, prima facie it seems reasonable for the privacy interests of the subject to prevail. Therefore, in such cases it should be relatively easy for a SEO to assess a delinking request. However, where the circumstances are not analogous the appropriate approach is less certain. In such a case, this paper submits that the suitable balance must be assessed based on the particular facts.

As discussed above, the ECJ proceeded on the basis that given the “potential seriousness” of the interference of a name-search there is essentially a presumption in favour of the data subject. The problem is that, in certain cases, there simply may not be such a risk of a serious interference. One such situation is where the subject has a particularly common name. For example a name-search on google.de for “Ben Müller”, the most common name in Germany,¹⁰⁷ produces over 32million search results.¹⁰⁸ In those circumstances, it seems unreasonable to assume that, prima facie, the nature of that name-search would constitute a serious interference for the particular applicant. Contrary to the view of the ECJ, in such a case it seems unlikely that the name-search would “establish a more or less detailed profile” of the relevant Ben Müller. Rather, any personal data about the particular applicant would likely exist in a disordered manner, littered amongst vast amounts of other personal information about individuals with the same name. Alternatively, even if a name-search does provide a “detailed profile” the interference may not be serious if the relevant results are difficult to locate; for example, if the relevant information on the particular Ben Müller exists after the 31st million result.¹⁰⁹ In these cases, the principle of proportionality demands a more critical assessment of the request for delinking.

¹⁰⁷ According to Wikipedia.

¹⁰⁸ As at 28 November 2014.

¹⁰⁹ Of particular relevance, evidence suggests internet users generally have little interest in looking beyond the first page of search results. See *Stuart*, above n2, p475.

There is also a concern as to how a SEO is to apply the qualifying criteria from *Google Spain*. It will be recalled from Part B that although a data subject's rights "override, as a general rule" those of internet users, the appropriate balance ultimately depends on the nature of the information, its sensitivity to the subject, the public's interest in the information and the role played by the subject in public life.¹¹⁰ While the succinct reference to these criteria is not particularly instructive, the following comment by the ECJ is even less enlightening:¹¹¹

...it should inter alia be examined whether the data subject has a right that the information in question relating to him personally should, at this point in time, no longer be linked to his name by a list of results displayed following a search made on the basis of his name...

These criteria are extremely subjective in nature, and require the SEO to make complicated value judgments about the merits of the application.¹¹² While SEOs and the A29 Working Party are currently developing guidelines,¹¹³ for the time being the vague criteria provided by the ECJ offer little assistance.

There are also potential complications in balancing the rights of website publishers. One such scenario is where the subject is seeking delinking of a sponsored link.¹¹⁴ In such a case, the publisher has actively exercised their rights to freedom of expression and business in paying for the link to appear, and the SEO has a particular economic interest in the

¹¹⁰ *Google Spain*, [81], and see also [97], [99].

¹¹¹ *Google Spain*, [96], [99].

¹¹² Depending on the circumstances, one difficulty with the assessment is the potential for it to be inherently paradoxical. For example, that a subject is requesting delinking of certain "irrelevant" information can in itself be seen as indicative that the information is likely relevant to someone else. Otherwise, what is the point of the request? However, this reasoning will not apply in all situations; for example, with respect to information which is merely embarrassing (such as nude photographs).

¹¹³ Article 29 Data Protection Working Party, *Press Release 6 June 2014* (Brussels).

¹¹⁴ This scenario is most likely to arise in the case of a name-search about a celebrity. In such a case, magazines or newspapers may invest in sponsored links so that their articles (personal data) about that person are listed first. See Stuart, above n2, p487-487.

maintenance of that link. Therefore, in such a delinking request there is a unique set of competing rights which must be taken into consideration.

Another scenario in which it may be particularly difficult to reconcile the rights of the subject with those of the publisher is where the relevant publisher has a unique justification for having their website linked to the name-search. While this may potentially arise in many respects – for example, a negative client review about a professional advisor – the nature of the principle is best demonstrated in an example where the publisher is a victim of a crime perpetrated by the data subject.¹¹⁵ Depending on the nature of the crime and when it occurred, applying the criteria in *Google Spain* it may be difficult to justify disclosure based on the interests of internet users – the information is likely to be particularly sensitive to the subject, and if the crime occurred a long time ago and re-offence is unlikely, there is limited public interest in access. However, the right to freedom of expression held by the victim publisher may strongly mitigate against delinking; for example, if the subject has recently chosen to write an article about the ongoing impact of the crime. It is not the intention of the present discussion to make a value judgment about the merits of delinking in such a case; as set out at the beginning of this Part C, this critical analysis is concerned with the *operation* of the right. Rather, the point being made is that in certain circumstances it may be difficult for a SEO to disregard the fundamental rights of the website publisher.

4.2.1.1.3 *Non-name searches*

Although the matter is subject to uncertainty,¹¹⁶ applying the Court’s approach in *Google Spain* it is in principle legally possible that a subject could require delinking of results in a non-name-search. In such a search, the SEO would still be a “controller” of the relevant processing.¹¹⁷ To the extent the presentation of the data in the search results is, *inter alia*,

¹¹⁵ Indeed, the very concept of a ‘right to be forgotten’ has traditionally found favour in this context, such as the French doctrine of “droit à l’oublié”: see Kulevska, above n80, p21; Shoor, above n49, p492.

¹¹⁶ *Google Spain* did not contemplate delinking from a non-name-search. To date, Google is not granting delinking with respect to non-name-searches, but will delink results from composite-name-searches. See Fleischer, Peter, *Submissions by Google to the Article 29 Working Party* (31 July 2014), p8-9.

¹¹⁷ See *Google Spain*, [28], [33].

inaccurate, irrelevant or excessive, conceptually the subject could object to the processing for non-compliance with the DPD.

In such a case, a question arises as to how the delinking request should be assessed. Compared to a name-search, the relevant distinction with a non-name-search is that the internet user is actively exercising their right to find information about a certain topic. With respect to the name-search in *Google Spain*, the ECJ stated that “in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a [name] search, access to that information”.¹¹⁸ By comparison, the context for a non-name-search is different; the user actively wants to find information about a certain topic. Therefore, that user is not directly trying to invade the subject’s privacy per se, but rather any such invasion is a mere indirect incidence of the user’s underlying factual pursuit. To the extent those search results are compromised, that may potentially constitute a significant interference with that user’s right to receive accurate and relevant information about the specific topic. Accordingly, arguably in the context of a non-name-search there *is* a more preponderant interest in the user having the information.¹¹⁹

4.2.1.2 The GDPR

As set out in Part B, it is difficult to assess the manner in which the right to delinking might operate under the GDPR because the final form of Article 17 remains uncertain. However, with this caveat established, it was concluded that since under both the DPD and GDPR the existence of the right appears to essentially turn on a balancing of competing fundamental rights, prima facie it seems likely that the right under the GDPR will operate in a similar to the DPD. Therefore, the discussion in the preceding subsection concerning the operation of the DPD can for the most part be considered equally applicable to the GDPR. That said, in

¹¹⁸ *Google Spain*, [98] (emphasis added).

¹¹⁹ This reasoning is, in principle, equally applicable in the context of a composite-name-search. However, a composite-name-search potentially represents a more serious interference with the privacy interests of the subject, in that it may be more likely to allow identification of the particular individual. One study found that 87 per cent of people in the US could be identified by a search using postal code, date of birth and sex. See: Ohm, Paul, ‘Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation’ (2010) 57 *UCLA Law Review* 1701, p1705; Kuner, above n7, p11.

view of the unique nature of the GDPR this section will provide a limited number of additional comments.

As discussed in Part B, the operation of GDPR Article 17(1) potentially provides an unqualified right to request delinking by a SEO, constrained by application of the exemption for freedom of expression in Article 17(3)(a). At least at one level, this creates a conceptually different framework compared to the DPD.¹²⁰ Under the DPD, it is possible to identify two distinct grounds for delinking arising from Articles 12(b) and 14(a). The first ground concerns erasure based on non-compliance with Article 6(1) because the processing is, *inter alia*, inaccurate, irrelevant or excessive.¹²¹ The second ground concerns erasure based on non-compliance with Article 7(f) because the legitimate interests of the SEO are overridden by the fundamental rights of the data subject.¹²² By comparison to this operation in the DPD, strictly speaking these two grounds are irrelevant under the GDPR; by reason of the unqualified right to request delinking, the request must be complied with unless retention is necessary for exercising the right to freedom of expression under Article 17(3)(a). Therefore, the approach under the GDPR is in some respects conceptually different – the focus is on freedom of expression, and it does not have the DPD’s explicit emphasis on the actual nature of the processing or the legitimate interests of the actual SEO as against the data subject.

It is unclear whether this conceptual difference might impact on the operation of the GDPR in practice. GDPR Article 17(3)(a) certainly contemplates that the conflicting interests be balanced, and this balancing should mostly entail consideration of the same issues that currently arise under the DPD. Indeed, compared to the uncertainty that exists under the DPD,¹²³ the broad reference to freedom of expression appears to explicitly permit consideration of the right to freedom of expression held by SEOs and website publishers. On the

¹²⁰ Mitchell-Rekrut, Cooper, ‘Search Engine liability under the LIBE Data Regulation Proposal’ (2014) 45 *Georgetown Journal of International Law* 862, p879.

¹²¹ Available under Article 12(b).

¹²² Available under Article 12(b) and Article 14(a).

¹²³ See above n95, n103.

other hand, the GDPR only explicitly contemplates balancing freedom of expression. This raises a question whether the legitimate business interests of SEOs or website publishers are to be considered. However, in this respect it is relevant that all EU laws are to be interpreted in view of the Charter,¹²⁴ which would involve consideration of the right to freedom of business. Furthermore, the doctrine of proportionality should demand consideration of the circumstances of the case.¹²⁵ This would include, inter alia, the economic impact of the delinking on the SEO and website publisher, and whether the actual search results were inadequate, excessive or no longer relevant. Therefore, ultimately the operation of the right under the GDPR may not be materially different to the DPD.

The final matter for consideration is that, under amended Article 17(3)(a) read in conjunction with Article 80, it is up to each Member State to provide the relevant exemption for freedom of expression. A concern here is that differing laws across Member States may jeopardise the Regulation's goal of harmonisation.¹²⁶ While it is unclear to what extent the ECJ will grant Member States a margin of appreciation in drafting the exemptions,¹²⁷ the history of implementing EU Directives suggests that in some cases there are likely to be material differences across different countries. If that is the case, the Californian company Google Inc will have to inform itself of any nuances across the individual freedom of expression laws of 28 different Member States. Indeed, it appears Google is already grappling with this problem.¹²⁸ This hardly creates a harmonised data protection framework, and potentially imposes significant compliance costs on SEOs, creates barriers to entry¹²⁹ and jeopardises the realisation of the single market.

¹²⁴ See, for example: Charter, Article 52; *Lindqvist*, above n103, [87].

¹²⁵ *Lindqvist*, above n103, [89].

¹²⁶ Shoor, above n49, p504.

¹²⁷ It is acknowledged that the various exemptions will need to respect the spirit of the regulation in accordance with the principle of proportionality: see *Lindqvist*, above n103, [87].

¹²⁸ Google's application form for lodging a request for delinking requires the applicant to "select a country so that we [Google] know which law to apply": see Fleischer, above n116, p2.

¹²⁹ See below, n182.

4.2.2 Should Google be the ringmaster?

In view of the above, assessing a request for delinking is a complex process that involves balancing a complicated distillation of competing fundamental rights. The complexity of this assessment, and the potential for divergence in opinion, is self-evident from the divergent views of the ECJ in *Google Spain* and the opinion of the AG. This raises a serious question as to whether a SEO, as a commercial entity, is capable of adequately performing this complex exercise.¹³⁰

The nature of the problem is heightened by the SEO's self interest in the outcome. While these matters are more fully explored below, in short complying with a delinking request imposes a direct and indirect cost on a SEO. On the other hand, incorrectly denying a request may also be extremely costly. Irrespective of the bias in the particular case, the important point is that a SEO is *not an impartial adjudicator*; 'no-one should be a judge in his own cause'. To some extent, this partiality may not be a significant concern for the data subject; if a subject feels a request was incorrectly denied, that subject can lodge an application with the relevant data protection authority. However, this partiality does potentially present a concern for the protection of freedom of expression. As a delinking request is a private matter between the SEO and subject, a request may be granted without notice to the relevant website publisher.¹³¹ Furthermore, internet users are only aware of the delinking to the extent the name-search results indicate that they have been edited.¹³² In these circumstances, the appropriate operation of the framework is extremely reliant on the potentially biased SEO conducting the assessment properly. Prima facie, this does not seem like an ideal regulatory model.

¹³⁰ House of Lords European Union Committee, *EU Data Protection law: a 'right to be forgotten'?* (2nd Report of Session 2014–15, Paper 40, 30 July 2014) ("HOL Report"), [56]. Kuner, above n7, p26.

¹³¹ Some commentators have noted that the ex-parte nature of this operation raises issues concerning a denial of natural justice for the publisher: see Brown, Ian (ed.), *Research Handbook on Governance of the Internet* (2013, Edward Elgar Publishing Limited), p294. However, Google uses its "Webmaster Tools" to notify the website of the delinking, and some publishers have subsequently complained about delinking, thereby mitigating this concern: Fleischer, above n116, p5-6.

¹³² A practice which Google does implement: Fleischer, above n116, p10.

A concern that follows from this operation is the potential for SEOs to remove search results without properly considering the merits of the request.¹³³ A number of factors give rise to this potential problem. The cost of ‘blindly’ complying with a request is likely to be minimal; a direct technical cost in removing the link, and a potential indirect cost in the form of the reduced custom. By comparison, the cost of fully assessing a request may be high; the potential complexity of balancing the competing interests was discussed above.¹³⁴ In the event the request is wrongly denied, the potential costs are even higher in the form of litigation costs and potential sanctions.¹³⁵ The net effect of the above is the propensity for the right to delinking to result in a practice of ‘blind takedowns’;¹³⁶ for a SEO, ‘if in doubt, take it out’. Such an outcome is inherently undesirable, as noted by the representative for Belgium at the recent JHAC Public Session:¹³⁷

There is a real risk, and it is not a negligible risk, that controllers, and in particular search engines, may decide to erase data in most cases, and that wouldn’t be a desirable outcome.

In this respect, it is useful to recall George Orwell’s famous words in *Nineteen Eighty-Four*; “Who controls the past controls the future. Who controls the present controls the past”.¹³⁸ In recognition of the potential for abuse, it is submitted that the framework needs to implement greater measures to ensure that important information is not inappropriately censored by those with a self-serving interest.¹³⁹ For example, during his infamous life

¹³³ However, to date it appears Google has been viewing delinking requests with reasonable scepticism. According to the *Telegraph*, as at October 2014 only 41.8 per cent of requested URLs have been removed. See ‘What people are asking to be removed from Google searches’, *The Telegraph* (online) 13 October 2014. See also, Fleischer, p11. Furthermore, in balancing the competing interests it appears Google is having regard to a wide range of relevant interests: See Fleischer, above n116, p4-5.

¹³⁴ Especially in the case of a ‘borderline’ request for delinking. See also, Alsenoy, above n 2, p65. In the case of the GDPR the problem is potentially even worse. Because the subject has an unqualified right to object and does not (compared to the DPD) need to, inter alia, provide “compelling legitimate grounds”, it may be particularly hard for a SEO to assess the merits of the objection.

¹³⁵ Shoor, above n49, p505, 507.

¹³⁶ Shoor, above n49, p512. See also Alsenoy, above n2, p64-65, 69.

¹³⁷ JHAC Public Session, above n58, around 1:11.20.

¹³⁸ Orwell, George, *Nineteen Eighty-Four* (2003, Penguin Books), p284.

¹³⁹ On this point, compare the opinion of Alsenoy, above n2, p72.

(1882-1949) Charles Ponzi committed numerous financial frauds in different jurisdictions, unimpeded by his long criminal history; after serving a custodial sentence in one state, he would simply move to another where his past indiscretions were unknown.¹⁴⁰ In recognising the right to delinking, caution must be exercised such that the utility of a name-search as a means to restrain the Charles Ponzis of the world is not inappropriately restrained. In this respect, Google has noted its reliance on the information provided by the applicant and that in some cases the requests have been based on “false and inaccurate information”.¹⁴¹ To ensure freedom of expression remains adequately protected, the operation of the current framework should be closely scrutinised to ensure the right to delinking is not being abused.¹⁴²

4.3 Search engines and “controllers”

As set out in Part B, based on *Google Spain* it appears settled that SEOs act as controllers when processing data in a name-search. With respect to the GDPR, the definition of controller is not materially different to the DPD in any way. Therefore, applying *Google Spain* it is possible that under the GDPR SEOs will also be considered controllers. However, in the GDPR the right to delinking is not contingent on this determination, since SEOs could potentially come within the scope of amended Article 17 as “third parties”. Accordingly, it is unclear how SEOs might be classified under the GDPR.

This section critically examines the concept of a SEO as a controller. In particular, the discussion will look at two main issues. Firstly, whether it is possible for a SEO to physically comply with the various obligations that are imposed on data controllers. Secondly, even if compliance is possible, whether the outcome is appropriate.

In view of the uncertainty as to how SEOs will be treated under the GDPR, in the event SEOs are deemed to be controllers the below discussion is applicable to both the DPD and

¹⁴⁰ Wikipedia, *Charles Ponzi*, accessed 1 December 2014.

¹⁴¹ Fleischer, above n116, p12.

¹⁴² See, for example, Alsenoy, above n2, p72; “the EU legislator would do well to consider the introduction of additional safeguards to mitigate the risk of excessive takedowns.”

GDPR. However, given the issues which will be explored this paper submits that there are strong arguments for SEOs to be treated as “third parties” under Article 17.

4.3.1 Can a SEO comply with the obligations on controllers?

Both the DPD and GDPR impose a number of obligations on controllers. Given the manner in which SEOs function, there is a question as to whether a SEO can reasonably comply with these obligations. While for present purposes it is unnecessary to outline the various obligations in detail, they are reasonably onerous and require, inter alia, that controllers: process data according to certain standards, including that the processing is fair and lawful, and adequate, relevant and not excessive;¹⁴³ process data legitimately, based on listed criteria such as consent;¹⁴⁴ only process certain ‘sensitive’ data in limited circumstances;¹⁴⁵ generally ensure the processing contains adequate levels of security;¹⁴⁶ generally provide data subjects with certain information concerning the processing;¹⁴⁷ grant data subjects a right of access to specific detailed information concerning the relevant processing.¹⁴⁸

As to the ability to comply with these obligations, the principal concern for a SEO stems from the fact that for the most part they passively process the personal data in automated systems, and do not exercise control over the data on the indexed website.¹⁴⁹ It is argued that such a modus operandi is at odds with the notion of a SEO as a controller, since on its proper interpretation the idea of a controller should be seen as a functional concept which is intended to allocate responsibility *where the factual influence is*¹⁵⁰ – the various obligations imposed on controllers contemplate the controller as an entity aware of the specific data processing that is taking place.¹⁵¹ So, for example, in his opinion in *Google Spain* the AG

¹⁴³ See DPD Article 6; GDPR, Article 5.

¹⁴⁴ See DPD Article 7; GDPR, Article 6.

¹⁴⁵ See DPD Article 8; GDPR, Articles 8, 9.

¹⁴⁶ See DPD Articles 16-17; GDPR, Articles 30-32.

¹⁴⁷ See DPD Articles 10-11; GDPR, Articles 11-14.

¹⁴⁸ See DPD Article 12; GDPR, Article 15.

¹⁴⁹ See generally, AG Opinion, above n27, [80]-[90].

¹⁵⁰ Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of “controller” and “processor”* (16 February 2010), p9. AG Opinion, above n27, [83], [88]. Alsenoy, above n2, p14-19.

¹⁵¹ AG Opinion, above n27, [82]-[83]. *Google Spain*, [22].

concluded that a SEO “cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data” on third party websites.¹⁵²

On the other hand, it is relevant that both the DPD and GDPR allow for considerable flexibility in their application. Both instruments contain a number of explicit exemptions, which allow for derogations from obligations where strict compliance would be disproportionate or unreasonable. Absent such exemptions, the principle of proportionality provides a basis for tailoring the obligations to the particular circumstances.¹⁵³ By applying either specific exemptions or the principle of proportionality, arguably it is possible for SEOs to comply with the various controller obligations. For present purposes it is unnecessary to specifically examine how every obligation can be so reconciled – that exercise has been undertaken in a paper by *Alsenoy*¹⁵⁴ – the important point is that it is at least possible.

4.3.2 Is it appropriate to treat a SEO as a controller?

Having established that SEOs may be able to fulfil the obligations of a controller, a question remains as to whether this outcome is appropriate. An issue arises because, in some instances, it is a relatively complex and convoluted process to reconcile the controller obligations with the manner in which SEOs operate.¹⁵⁵ In such cases, there is a concern that the relevant obligations risk becoming ‘empty shells’ – if a reasonable interpretation of a

¹⁵² AG Opinion, above n27, [89].

¹⁵³ Alsenoy, above n2, p28. Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (20 June 2007) (“A29 Opinion 4/2007”), p4-5.

¹⁵⁴ See Alsenoy, above n2, p28-45.

¹⁵⁵ For example, DPD Article 12(a) and GDPR amended Article 15(1)(c) give the data subject the right to obtain from the controller information as to the recipients of the data. Neither provision contains a specific exemption. For a SEO this raises a complicated question as to whether they are obligated to provide information about who has searched that data subject’s name, since most SEOs maintain logs of prior search results. Such an obligation could create complicated privacy problems – while it is unclear in the EU whether IP addresses constitute personal data, there is authority suggesting they are – such that disclosing this information would itself have serious privacy implications. While based on the principle of proportionality it can be argued that the appropriate SEOs should therefore not provide such information, the example highlights the potential complexity faced by an SEO as a controller. See Alsenoy, above n2, p39. Regarding IP addresses as personal data, see: A29 Opinion, above n153, p16-17; *Promusicae v Telefonica*, ECJ Case no. C-275/06, [45]; *Scarlet Extended v SABAM*, ECJ Case no C-70/10, [51]; compared to *EMI Records v Eircom* [2010] IEHC 108 [24]-[25].

SEO's obligations as a controller de facto exempts them from (proactively) complying with several key principles, this could undermine the nature of the framework as a whole.¹⁵⁶

The European Commission's response to this concern appears to be that a SEO's obligations should be assessed on a case-by-case basis, in the context of specific requests.¹⁵⁷ To this effect, *Google Spain* can be seen as a decision specifically concerned with the right to require delinking, and does not therefore have broader implications such that a SEO must immediately comply with all controller obligations. Despite its convenience, the problem with this approach is that it creates considerable legal uncertainty for SEOs as to what their obligations actually are. While over time further guidance may become available, for example in the form of ECJ judgments or opinions of the Article 29 Working Party, in the interim period this situation is arguably unsatisfactory.

The general nature of this problem arises because of the broad language used in the DPD. Indeed, given the broad definition of "controller" it is difficult at one level to criticise the judgment in *Google Spain* as legally incorrect; SEOs do satisfy the relevant criteria for a controller at least in a formal sense.¹⁵⁸ However, arguably this result is merely the product of EU regulation; operating as supra legislation, EU instruments deliberately use broad language to allow for a flexible application depending on the facts of the case.¹⁵⁹ On that basis, the real question is not whether the interpretation is legally justified in a strict sense, but rather whether it is a reasonable and proportionate interpretation in the circumstances.

In this respect, *Google Spain* can be criticised as overly formalistic. For example, the AG commented that while deeming SEOs as controllers "might easily be defended as a logical conclusion of a literal and perhaps even teleological interpretation of the Directive" such an approach "completely ignores" that when the DPD was drafted it was not possible to fore-

¹⁵⁶ Alsenoy, above n2, p44.

¹⁵⁷ Alsenoy, above n2, p44.

¹⁵⁸ See Alsenoy, above n2, p16. For example, a UK House of Lords enquiry canvassed opinions from prominent commentators and the majority accepted the judgment was legally acceptable: HOL Report, above n130, [27]-[29].

¹⁵⁹ Druschel, Peter, Michael Backes and Rodica Tirtea, *The right to be forgotten – between expectations and practice* (European Network and Information Security Agency, 20 November 2012), p7.

see the full emergence of the internet.¹⁶⁰ The AG cautioned that, if SEOs were treated as controllers, such a broad interpretation could cover “virtually everybody owning a smartphone or a tablet or laptop computer”.¹⁶¹ He reasoned that such an outcome demonstrated the “irrational nature of the blind literal interpretation of the Directive in the context of the internet,”¹⁶² and accordingly submitted that a reasonable and proportionate interpretation demanded that a SEO not be considered a controller.¹⁶³ Clearly, the ECJ did not agree.

In view of the above concerns about an overly broad interpretation of “controller”, it is submitted that the approach in *Google Spain* must be seen as arising from, and limited to, the facts of that case. So, in the case of a name-search, according to the ECJ it was appropriate that a SEO be considered a controller because its activities were “liable to affect significantly, and additionally compared with that of the publishers of websites” the privacy interests of the subject.¹⁶⁴ However, in other cases there may not be this requisite significant and additional interference with privacy; for example, in the case of the AG’s concerns about a “smartphone or a tablet or laptop computer”. On this line of argument, what is unfortunate about the Court’s approach is not that it was wrong, but that we become only incrementally closer to answering the fundamental question; when exactly is an entity a controller, and what are its obligations?

4.3.3 Interim conclusion on the controller question

Ultimately, what becomes apparent from the above discussion is that defining a SEO as a controller, while workable, is problematic. These problems arise because, given their relatively unique activities, SEOs simply don’t fit neatly with the notion of a controller. Therefore, putting aside any debate about the merits of a right to delinking, with respect to the *operation* of that right it is submitted that SEOs should be treated as unique entities. While

¹⁶⁰ AG Opinion, above n27, [77].

¹⁶¹ Ibid, [81]. Accordingly, the AG submitted that the doctrine of proportionality should be applied in order to avoid unreasonable and excessive legal consequences: AG Opinion, above n27, [30], [79].

¹⁶² AG Opinion, above n27, [81].

¹⁶³ Ibid, [89].

¹⁶⁴ *Google Spain*, [38].

Google Spain may have cemented a contrary position under the DPD, with respect to the GDPR the reference to “third parties” in amended Articles 17(1) and 17(3) provides the ideal avenue for such an approach. By treating SEOs as third parties the full effect of the right to delinking would be preserved, without any of the above complications which arise from treating a SEO as a controller; it is a “win-win” approach. Therefore, it is strongly submitted in this respect that the amended versions of Articles 17(1) and 17(3) should be preferred, and that under the GDPR SEOs should be treated as “third parties”.

4.4 Extra-territoriality and non-EU search engines

Both the DPD and GDPR seek to have extra-territorial effect outside of the EU in certain cases. This issue has received considerably scholarly attention. In short, some commentators express concern about over-reach by the legislation giving rise to various legal problems with enforcement, conflicts of laws and interference with territorial sovereignty. On the other hand, proponents of the extra-territorial reach argue that EU States must try and protect the privacy of their citizens from abroad, and that the situation is analogous to compliance by any foreign company that wishes to operate in an EU jurisdiction.¹⁶⁵ In any event, a full analysis is beyond the present scope; rather, what is important is whether this extra-territorial operation is satisfactory with respect to the right to delinking.

The discussion is again best illustrated with reference to Google. The California based company Google Inc is responsible for Google Search. Google Search includes local EU versions such as google.es, and also ‘foreign’ non-EU versions such as google.com. While both versions are likely to be accessible within the EU, the local versions are specifically ‘geared’ towards the relevant EU Member State; inter alia, they are tailored to the local language,¹⁶⁶ and provide search results based on the users location.¹⁶⁷

¹⁶⁵ Alsenoy, above n2, p22-23.

¹⁶⁶ *Google Spain*, [43].

¹⁶⁷ Google tailors its search results depending on the user’s location. For example, a search for ‘plumber’ on google.uk will tend to give results for UK based plumbers.

Potentially, the operation of Google Search does not involve any processing of personal data in the EU; while the exact location of Google Inc’s data centres is a secret, for the purposes of *Google Spain* it was established that no processing of personal data relating to Google Search took place in Spain,¹⁶⁸ and it is possible that no processing takes place in the EU. In these circumstances, the operation of the DPD and GDPR on Google Search may always depend on their extra-territorial provisions. Following *Google Spain*, based on the “establishment” criterion in DPD Article 4 it appears that local versions of Google Search will need to comply with the Directive.¹⁶⁹

While this resolves the operation with respect to local EU versions of Google Search, there remains a more complicated issue concerning the right to delinking against foreign versions such as google.com. Indeed, the fact that Google has not yet applied erasure beyond the local versions has led to some criticism that Google is evading the ECJ ruling.¹⁷⁰ Given the broad meaning of “establishment” and “equipment”,¹⁷¹ potentially a citizen of the EU¹⁷² may seek delinking from the search results of a foreign version of the search engine. Such an application may be attractive if the foreign version is popular in the EU,¹⁷³ or where a particular SEO does not operate a local EU version in which case the foreign search engine would be the only possible target for enforcement.¹⁷⁴ In the event a subject approached a European Court with such an application, there are essentially three potential outcomes: the application could be denied; the request could be upheld; the foreign SEO could be ordered

¹⁶⁸ AG Opinion, above n27, [62]. Alsenoy, above n2, p26. *Google Spain*, [43].

¹⁶⁹ It appears that the outcome will be the same under the GDPR; for the purpose of the present discussion, the wording of the analogous GDPR Article 3 is not materially different from DPD Article 4.

¹⁷⁰ Peltz-Steele, above n81.

¹⁷¹ Potentially, given that a SEO ‘crawls’ EU servers for webpages the notion of “equipment” could capture a SEO which did not otherwise meet the “establishment” criterion in DPD Article 4. See Alsenoy, above n2, p26. However, it is acknowledged that the “equipment” criterion has been removed in the GDPR. See EU Parliament Resolution, above n6, Amendment 97.

¹⁷² Interestingly, Kuner notes that the right is potentially also open to any citizen around the world: Kuner, above n7, p14-15. However, Google is currently applying the right on the basis that “individuals will need some connection to that [EU] country”: Fleischer, above n116, p7.

¹⁷³ However, Google actively redirects European users from google.com to the local EU versions, with the result that fewer than 5 per cent of European users use google.com: Fleischer, above n116, p3-4.

¹⁷⁴ However, Google Search has a local version in every EU Member State.

to tailor the search results it provides to citizens of the EU. Each possibility will be considered in turn.

If the right to delinking doesn't apply to foreign search engines, the extra-territorial effect of the regulation is clearly restricted. While this deals with the legal concerns that arise from extra-territorial laws, the risk is that it may render the EU regulations relatively worthless; EU citizens could simply use the foreign search engine. This concern is less prevalent where users have a strong preference for the local version. This may be because it provides more useful search results given the type of search request, or because language barriers exist; for example, for some internet searches Norwegian citizens may be relatively loyal to google.no for linguistic reasons. However, in cases where the foreign search engine is a suitable substitute the operation of the regulation may be severely compromised. In the context of a name-search, this may be the case if the subject has a particularly unique name, such that the results provided by a foreign version of Google Search are just as relevant as the results in the local version.¹⁷⁵

On the other hand, it seems entirely inappropriate for the right to apply to all foreign search engines. There are likely to be (substantial) difficulties in enforcing such a broad operation, as foreign courts are unlikely to recognise the European law. Perhaps most importantly, in the case of lawfully published information US Courts will almost certainly not recognise the EU right to erasure against google.com.¹⁷⁶ More broadly, it is also important to recognise that Europe is not the policeman of the internet, and the EU must recognise the legal sovereignty of other countries to regulate their online affairs even though such foreign content may be accessible in Europe. This is especially so since the right to erasure is not one which is widely recognised by other countries, and therefore for which there is a degree of

¹⁷⁵ In this respect, it is important to recognise that all versions of Google Search can potentially use the same 'index', and therefore provide the same results. To the extent a local version provides different results, that may often relate to the ranking of webpages, as opposed to what webpages actually make up the search results as a whole.

¹⁷⁶ See Stuart, above n2, p487-492. Larson, Robert, 'Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech' (2013) 18(1) *Communication Law and Policy* 91, p120.

‘consensus authority’ – in this sense it is not analogous to, for example, online protection of intellectual property rights, a matter on which many countries are signatories to the relevant conventions and treaties.¹⁷⁷

The third possibility would be to require foreign search engines to restrict the results they provide to EU citizens. So, for example, in order to comply with the EU regulations google.com would provide different search results to French citizens as compared to US users. The notion is not entirely new. As part of the Yahoo! case in France an investigation found that Yahoo! had the capability to block up to 90% of French users from accessing the offending content on the US website.¹⁷⁸ However, there are a number of problems. In view of the preceding paragraph, there would be a question as to whether such a requirement could be legally enforced against the likes of google.com. Furthermore, technical capabilities remain limited; among other techniques, VPN’s can easily mask a user’s country of origin. Also, the technological and economic burden of compliance would need to be appropriately balanced.

For the time being, it appears reasonably settled that the EU right to delinking only applies to local EU versions of search engines. In this sense, it is somewhat fortuitous that Google offers local versions of Google Search in every Member State; one can only imagine the complexity of the present discussion if all countries used google.com. But the matter should not be considered definitely settled, especially in the long run. There are numerous examples outside of the right to erasure where EU citizens have sought to enforce EU privacy or intellectual property standards on US internet companies.¹⁷⁹ While such actions have generally had only limited success, the concern in the case of Google Inc is that the company potentially has significant assets within the EU jurisdiction capable of attach-

¹⁷⁷ See Edwards & Waelde (eds.) *Law and the Internet* (2009, Oxford and Portland, Hart Publishing), p188.

¹⁷⁸ Ibid, p59-60; Reed, Chris, *Making Laws for Cyberspace* (Oxford University Press, 2012), p14. This consideration may be particularly relevant if a SEO, instead of offering local versions of its search function, provided only one global URL but tailored its search results based on the location of the search request.

¹⁷⁹ See, for example, the “Wikipedia case”: Shoor, above n49, p493. See also: Schwartz, John, ‘Two German Killers Demanding Anonymity Sue Wikipedia’s Parent’, *The New York Times* (online) 12 November 2009.

ment.¹⁸⁰ Nevertheless, it is submitted that European Courts must not attempt to enforce delinking from the likes of google.com; doing so would constitute an intolerable violation of US sovereignty, and would potentially create a transatlantic clash of unprecedented scale with respect to online regulation.

4.5 Economic considerations

This section will briefly consider the potential economic impacts of the EU recognising a right to delinking. The discussion does not attempt to provide any form of comprehensive economic analysis for or against the right to delinking. Rather, the more limited purpose is merely to highlight the potential impacts and caution against implementing potentially burdensome privacy protection measures without proper consideration of the economic implications.

The right to delinking is not recognised in a number of important technology markets, in particular the US. For the EU, this raises a concern about whether the introduction of the right might place the Union at a competitive disadvantage in attracting investment from existing SEOs, and in facilitating the start-up of new European based SEOs. Broadly speaking, complying with the right to delinking imposes a direct and indirect cost on a SEO. There is a direct economic cost in physically dealing with the delinking requests. For example, in the month of June 2014 Google received more than 70,000 removal requests, with an average of 3.8 URLs per request. That means that Google must review over a quarter of a million URLs and assess in each case, on the basis of the complicated criteria discussed above, whether delinking is required.¹⁸¹ In the event Google gets that assessment wrong, or the outcome is in any event challenged, there is also the potential for litigation costs and sanctions. As to indirect costs, if relevant search results are delinked users may switch to an alternative SEO and thereby reduce Google's ability to attract advertising revenue.

¹⁸⁰ Although it appears many of those assets are held by subsidiary companies, thereby raising questions about the extent to which a judgment can be enforced.

¹⁸¹ HOL Report, above n130, [33].

In view of these costs, there becomes an economic incentive for a SEO to structure their operations to avoid the EU right to delinking. For example, Google Inc could potentially avoid the regulation by no longer offering local EU versions of Google Search. Alternatively, a SEO may decide to only provide a local version in countries where the economic benefits outweigh the cost of complying with the right to delinking.¹⁸² And, given the potential for extremely large fines under the GDPR,¹⁸³ a SEO may consider it prudent to limit its EU exposure by removing, protecting or not investing further in EU based assets. Ultimately, it is a question for each SEO as to how it wishes to structure its operations in view of the EU regulation, and this paper will not indulge in the many hypothetical possibilities. For very large companies like Google, Bing or Yahoo!, in all likelihood the existence of the right to delinking will not warrant any dramatic change in their business structure.¹⁸⁴ However, for a small SEO contemplating entry into the European market through the offering of local EU versions of its search function, or deciding in which country it wishes to establish an office or data centres, the potential for avoiding the regulation may carry greater weight.¹⁸⁵

There is also the potential for the right to operate discriminately against large SEOs, notably Google. This is because, given its overwhelming market share, in many cases a subject may only consider it necessary to pursue delinking from Google Search. Indeed, at least in the primary action apparently Mr Gonzalez did not feel it necessary to proceed against Yahoo! or Bing. While this may not be unfair – Google is well placed to deal with the burden with a market capitalisation of over USD400 billion, – it is unjust. To the extent various

¹⁸² Take, for example, Malta. According to Wikipedia, it is the smallest EU state with a population of only approximately 420,000, it is only ranked 12th in terms of GDP per capita (at around EU27,000), and English is widely spoken (meaning other English versions of the search engine might be suitable substitutes): see Wikipedia, *Member State of the European Union* (accessed 1 December 2014). For Bing or Yahoo!, with an average global market share of around 4 per cent (see Stuart, above n11), the market therefore potentially represents a mere 16,800 Maltese customers each. Nevertheless, to comply with the GDPR they must inform themselves of Malta’s provisions for freedom of expression and provide a means for Maltese citizens to request delinking.

¹⁸³ Potentially a fine up to 5 per cent of the SEOs “annual worldwide turnover”: see GDPR, amended Article 79(2a)(c).

¹⁸⁴ Indeed, Google has not responded as such following *Google Spain*.

¹⁸⁵ A House of Lords enquiry expressed concerns that the costs of compliance with the GDPR “might result in many SMEs not getting beyond the start-up phase”; HOL Report, above n130, [43].

other SEOs are also contravening EU data protection laws, arguably equity demands that they also be required to comply with the regulations.

However, there are concerns to the extent delinking requests are directed at small SEOs. The cost of compliance represents a potential barrier to entry. There is also a concern that, as a small company, inadequate resources may prevent a proper assessment of the request and therefore result in ‘blind’ delinking.¹⁸⁶ By comparison, a large SEO which can afford to properly assess each request may end up retaining a greater number of search results, cementing its competitive advantage. Taken together, these outcomes are potentially economically undesirable for a market already heavily dominated by one participant.

Notwithstanding these concerns, the potential for economic benefits is also acknowledged. A key rationale behind the introduction of the GDPR is the need to protect consumer confidence in the digital market, and thereby foster further economic growth.¹⁸⁷ Indeed, there appears to be popular support for a right to erasure among European nationals; a 2011 survey revealed that 75 per cent of Europeans want to be able to delete personal information online whenever they want.¹⁸⁸ Therefore, if the regulation results in more people using the services of SEOs, this may mitigate against the above concerns.

Ultimately, it remains to be seen whether the potential economic costs of the right to delinking will have a negative effect on the European market. For the time being, the SEOs seem content to comply with the regulation without altering their operations. Furthermore, as a highly concentrated market characterised by a few large market participants, at least in the current circumstances concerns about the impact of the right on small SEOs seem negligible. That said, regulation is not without cost. This should always be kept in mind, especially with respect to potentially costly regulatory measures which will not be implemented

¹⁸⁶ Ibid, [35].

¹⁸⁷ European Commission, *Press conference by Viviane Reding on the Data Protection Proposal* (Video of Press Conference, European Commission Audio-visual Services, 25 January 2012), at 1.55. European Commission, *How will the data protection reform affect social networks?* (European Commission Fact Sheet).

¹⁸⁸ European Commission, *European Commission – Press Release – Data Protection: Europeans share data online, but privacy concerns remain – new survey* (16 June 2011).

in the markets of competitor nations. This is perhaps even more important with respect to a law which at its foundation is concerned with protecting privacy as a fundamental right; because, by its very nature, a fundamental right can be given an infinite value, the potential for a cost-benefit analysis can be inappropriately restricted notwithstanding that it is entirely warranted.¹⁸⁹ While privacy is undoubtedly an important fundamental right, it is not appropriate for privacy regulation to be contemplated in an economic vacuum.

5 CONCLUSION

On first hearing of the right to delinking, there is a propensity to view the concept with much scepticism. Why should someone have the right to delete a link to legally published, truthful information – if it was rightfully published, why shouldn't you have the right to readily access it via a search enquiry? It is, after all, merely a statement of truth. However, on further contemplation the issue reveals its true complexity. In the end, the right is not contemplating that old books be burnt in the street or that someone have the power to rewrite the past. Rather, it is dealing with a unique problem that arises from the now ubiquitous internet; how do we deal with the serious threat to privacy posed by search engine results?

When the full nature of this unique threat is contemplated, the very notion of a right to delinking becomes entirely less offensive. In the modern era there are becoming too many examples of intolerable abuses of privacy. *Stuart* notes two poignant illustrations from the US, where a right to delinking is not recognised: an intrusive video of a sports-caster which was originally uploaded by a stalker and which, notwithstanding numerous attempts over several years, remains a top result to the sports-caster's name-search; mugshot websites which publicise arrest photos and demand a fee for their removal, which by reason of their popularity result in the relevant photos featuring prominently in a name-search.¹⁹⁰ In such

¹⁸⁹ Shaffer, Gregory, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) 25 *Yale Journal of International Law* 1, p19.

¹⁹⁰ *Stuart*, above n2, p486, 502-503, 511.

cases, it is hard to reasonably argue against some form of greater protection for personal privacy.

So, what then of the EU right to delinking? Save for the indulgent comments in the preceding paragraph, this paper undertook to critically examine the right in view of the manner in which it *operates*; whether the framework adequately balances the various conflicting fundamental rights, and whether it could be applied in a practical, equitable, efficient and certain manner. In view of this criteria, ultimately this paper has submitted that there are serious deficiencies with the current framework. In particular, the discussion raised concerns about, inter alia, the approach adopted by the ECJ in *Google Spain*, that SEOs may not properly deal with requests for delinking, and that it is inappropriate to treat SEOs as controllers. However, it is acknowledged that to some extent these concerns may turn out to be temporary; the creation of better guidelines for SEOs to assess delinking requests will help ensure an appropriate balancing of rights, and under the GDPR there is the potential for SEOs to be treated as “third parties”.

However, perhaps the most promising addition to the debate comes from the conduct of Google itself in the few months that have passed since the decision in *Google Spain* was handed down. The company has not thumbed its nose at the ruling, but appears to be diligently trying to work through the thousands of requests it has received. And, most importantly, it appears to be taking a well-reasoned, proportionate approach in its assessment – results concerning matters such as botched medical procedures, and recent arrests for financial crimes, remain (rightly) linked – results concerning matters such as spent criminal convictions, and conduct that occurred as a minor, have been (rightly) delinked.¹⁹¹ It would appear that, at least for some, it may be possible to live by Elizabeth Darcy’s philosophy after all.

¹⁹¹ The Telegraph, above n133.

6 Table of reference

Articles, Books, Reports

Austen, Jane, *Pride and Prejudice*, (1853, RD Bentley), p323

Baker, Michael and Alan Westin, *Databanks in a Free Society; Computers, Record-Keeping, and Privacy* (1972, Quadrangle Books)

Brin, Sergey and Lawrence Page, 'The anatomy of a large-scale hypertextual Web search engine' (1998) 30 *Computer Networks and ISDN Systems* 107
<<http://snap.stanford.edu/class/cs224w-readings/Brin98Anatomy.pdf>>

Brown, Ian (ed.), *Research Handbook on Governance of the Internet* (2013, Edward Elgar Publishing Limited)

Bygrave, Lee, *Data Privacy Law – An International Perspective* (Oxford University Press, 2014)

Edwards & Waelde (eds.) *Law and the Internet* (2009, Oxford and Portland, Hart Publishing)

European Commission, 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data' (23 November 1995) No. L281 *Official Journal of the European Union* 31-50

European Commission, 'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce)' (17 July 2000) No. 178 *Official Journal of the European Union* 1-16

Larson, Robert, 'Forgetting the First Amendment: How Obscurity-Based Privacy and a Right to Be Forgotten Are Incompatible with Free Speech' (2013) 18(1) *Communication Law and Policy* 91

McNealy, Jasmine, 'The Emerging Conflict Between Newsworthiness and the Right to be Forgotten' (2012) 39(2) *Northern Kentucky Law Review* 119

Mitchell-Rekrut, Cooper, 'Search Engine liability under the LIBE Data Regulation Proposal: Interpreting third party responsibilities as informed by *Google Spain*' (2014) 45 *Georgetown Journal of International Law* 862

Ohm, Paul, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymisation' (2010) *57 UCLA Law Review* 1701

Orwell, George, *1984* (2003, Penguin Books)

Reed, Chris, *Making Laws for Cyberspace* (Oxford University Press, 2012)

Shaffer, Gregory, 'Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards' (2000) *25 Yale Journal of International Law* 1

Shoor, Emily, 'Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation' (2014) *39(1) Brooklyn Journal of International Law* 487

Stuart, Allyson, 'Google Search Results: Buried if not Forgotten' (Spring 2014) *15(3) North Carolina Journal of Law & Technology* 463

Cases

Bodil Lindqvist, ECJ Case no. C-101/01, 6 November 2003

EMI Records v Eircom [2010] IEHC 108

Google Spain SL & Anor v AEPD & Anor, ECJ Case no. C-131/12, 13 May 2014

Österreichischer Rundfunk v. Austria, ECtHR Case no. 35841/02, 7 December 2006

Promusicae v Telefonica, ECJ Case No. C-275/06, 29 January 2008

Satakunnan Markkinapörssi and Satamedia, ECJ Case no. C-73/07, 16 December 2008

Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen, ECJ Cases nos. C-92/09 and C-93/09, 9 November 2010

Other

Advocate General Jääskinen, *Opinion of Advocate General Jääskinen delivered 25 June 2013 – Case C-131/12 – Google Spain SL & Anor v AEPD & Anor* (25 June 2013)
<<http://curia.europa.eu/juris/document/document.jsf?docid=138782&doclang=EN>>

Albrecht, Jan Philipp, *Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Report A7-0402/2013* (21 November 2013)

<<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//EN>>

Alsenoy, Van, Aleksandra Kuczerawy and Jef Ausloos, *Search Engines after 'Google Spain': Internet@Liberty or Privacy@Peril?* (ICRI Research Paper 15, TPRC 41: The 41st Research Conference on Communication, Information and Internet Policy, University of Leuven, 6 September 2013)

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2321494>

Article 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data* (20 June 2007)

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf>

Article 29 Data Protection Working Party, *Opinion 1/2010 on the concepts of “controller” and “processor”* (16 February 2010)

<http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf>

Article 29 Data Protection Working Party, *Press Release 6 June 2014* (Brussels)

<http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/20140606_wp29_press_release_google_judgment_en.pdf>

Council of the European Union, *Justice and Home Affairs Council – Public Session, Friday, October 10, 2014 at 10:10am* (Webcast, 10 October 2014)

<<http://video.consilium.europa.eu/webcast.aspx?ticket=775-979-14911>>

Cuijpers, Colette, Nadezhda Purtova and Eleni Kosta, *Data Protection Reform and the Internet: The Draft Data Protection Regulation* (Tilburg Law School Legal Studies Research Paper Series No.03/2014, Tilburg University, 2014)

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2373683>

Druschel, Peter, Michael Backes and Rodica Tirtea, *The right to be forgotten – between expectations and practice* (European Network and Information Security Agency, 20 November 2012)

<<http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/the-right-to-be-forgotten?searchterm=forgotten>>

European Commission, *Application of EU law – What are EU Regulations?* (25 June 2012)

<http://ec.europa.eu/eu_law/introduction/what_regulation_en.htm>

European Commission, *Factsheet on the “Right to be Forgotten ruling” (C-131/12)*

<http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf>

European Commission, *Press Release – Data Protection: Europeans share data online, but privacy concerns remain – new survey* (16 June 2011)

<http://europa.eu/rapid/press-release_IP-11-742_en.htm>

European Commission, *Press release - Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses* (25 January 2012) <http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en>

European Commission, *Press conference by Viviane Reding on the Data Protection Proposal* (Video of Press Conference, European Commission Audio-visual Services, 25 January 2012)
<<http://ec.europa.eu/avservices/video/player.cfm?ref=82655>>

European Commission, *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (Brussels, 25 January 2012)
<http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

European Commission, *Memo/14/60 – Data Protection Day: Full Speed on EU Data Protection Reform* (European Commission Memo, European Commission Strasbourg, 27 January 2014)
<http://europa.eu/rapid/press-release_MEMO-14-60_en.htm>

European Commission, *Memo/14/186 - Progress on EU data protection reform now irreversible following European Parliament vote* (European Commission Memo, European Commission Strasbourg, 12 March 2014)
<http://europa.eu/rapid/press-release_MEMO-14-186_en.htm>

European Commission, *How will the data protection reform affect social networks?* (European Commission Fact Sheet)
<http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/3_en.pdf>

European Parliament, *European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (12 March 2014)
<<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN>>

European Parliament, *Press Release – MEPs tighten up rules to protect personal data in the digital era* (12 March 2014)
<<http://www.europarl.europa.eu/news/en/news-room/content/20140307IPR38204/html/MEPs-tighten-up-rules-to-protect-personal-data-in-the-digital-era>>

Fleischer, Peter, *Submissions by Google to the Article 29 Working Party* (31 July 2014)

<<http://online.wsj.com/public/resources/documents/google.pdf>>

Google, *Inside Search – How Search Works*

<<http://www.google.com/insidesearch/howsearchworks/thestory/>>

House of Lords European Union Committee, *EU Data Protection law: a ‘right to be forgotten’?* (2nd Report of Session 2014–15, Paper 40, 30 July 2014)

<<http://www.publications.parliament.uk/pa/ld201415/ldselect/ldeucom/40/40.pdf>>

House of Lords European Union Committee, *EU Data Protection law: a ‘right to be forgotten’? Evidence* (July 2014)

<<http://www.parliament.uk/documents/lords-committees/eu-sub-com-f/righttobeforgotten/right-to-be-forgotten-evidence.pdf>>

Kulevska, Sanna, *Humanizing the Digital Age: A Right to be Forgotten Online? – An EU-U.S. Comparative Study of Tomorrow’s Privacy in Light of the General Data Protection Regulation and Google Spain v. AEPD* (LLM Graduate Thesis, Lund University, May 2014)

<<http://lup.lub.lu.se/luur/download?func=downloadFile&recordOid=4449685&fileOid=4610795>>

Kuner, Christopher, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines: Current Issues and Future Challenges* (15 September 2014)

<http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2496060>

Peltz-Steele, Richard, 'Right to be forgotten' is effectively a right to be forgiven, *The Sydney Morning Herald* (Online) 24 November 2014

<<http://www.smh.com.au/digital-life/digital-life-news/right-to-be-forgotten-is-effectively-a-right-to-be-forgiven-20141123-11sg8n.html>>

Schwartz, John, 'Two German Killers Demanding Anonymity Sue Wikipedia’s Parent', *The New York Times* (online) 12 November 2009

<<http://www.nytimes.com/2009/11/13/us/13wiki.html>>

The Telegraph, 'What people are asking to be removed from Google searches', *The Telegraph* (online) 13 October 2014

<<http://www.telegraph.co.uk/technology/google/11157003/What-people-are-asking-to-be-removed-from-Google-searches.html>>

Wikipedia, *Charles Ponzi* (accessed 1 December 10)

<http://en.wikipedia.org/wiki/Charles_Ponzi>

Wikipedia, *Member State of the European Union* (accessed 1 December 2014)

<http://en.wikipedia.org/wiki/Member_state_of_the_European_Union>