PERSONAL DATA DOWN THE MEMORY HOLE:

SEARCH ENGINE OPERATOR LIABILITY IN EUROPEAN DATA PROTECTION LAW

Ella Florencia Collis

A dissertation submitted in partial fulfilment of the degree of Bachelor of Laws (Honours) at the University of Otago – Te Whare Wānanga o Otāgo.

9 October 2015

Acknowledgements

To my supervisor, Paul Roth, for his support and guidance.

To my parents, Steven and Trish, for their love and encouragement.

And to Yasmin and Jessica, for keeping me sane.

Abbreviations

A29WP	Article 29 Working Party
CJEU	Court of Justice of the European Union
DPD	Data Protection Directive
GDPR	General Data Protection Regulation
EU	European Union
SEO	Search Engine Operator

Table of contents

INTRODUCTION

> It was very difficult for him to sleep. To sleep is to be abstracted from the world; Funes, on his back in his cot, in the shadows, imagined every crevice and every molding of the various houses, which surrounded him. (I repeat, the least important of his recollections was more minutely precise and more lively than our perception of a physical pleasure or a physical torment).
>
> - Jorge Luis Borges, *Funes the Memorious*.[1]

> [H]e crumpled up the original message and any notes that he himself had made, and dropped them into the memory hole to be devoured by the flames.[2]
>
> And somewhere or other, quite anonymous, there were the directing brains who co-ordinated the whole effort and laid down the lines of policy which made it necessary that this fragment of the past should be preserved, that one falsified, and the other rubbed out of existence.[3]
>
> - George Orwell, *1984*.

Forgetting is an essential characteristic of the human memory. We have neither the massive storage capabilities nor incredible retrieval systems required to archive and recall each and every sensation, thought and event we have experienced.[4] However, the digital age has shifted our 'societal default' from forgetting to remembering, much like that which has happened to Borges' character.[5]

The Internet has been described as enabling the details of our lives to be kept "relentlessly in focus, for everyone, forever."[6] This tendency of the Internet to remember can seriously impact upon the moral right of a person to freely

---

[1] For Ireneo Funes, the fictional character of Jorge Luis Borges' novel, the present has lost all meaning because he is forever consumed by his memories of the past: Jorge Luis Borges *Funes el Memorioso* (Emece Editores, Argentia, 1956) (translated ed: Anthony Kerrigan (translator) Jorge Luis Borges *Ficciones* (Grove Press, New York, 1962) at 103.
[2] George Orwell *1984* (Harcourt Brace Jovanovich, New York, 1949) at 40.
[3] At 43.
[4] Allen Baddeley *Human Memory: Theory and Practice* (Revised ed, Psychology Press Ltd, Bristol, 1997) at 5.
[5] Viktor Mayer-Schönberger "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing" (Faculty Research Working Papers Series No. 22, John F.Kennedy School of Government - Harvard University, 2014) at 7.
[6] Lev Grossman "You Have the Right to Be Forgotten" *TIME* (online ed, New York, 26 May 2014) at 17.

develop a personal identity. The value in protecting one's privacy online is becoming increasingly perceived. It may be necessary to import the humanistic tendency to forget back into the digital environment so as to give back to individuals a greater degree of control over their personal data. However, this will detrimentally affect values such as the right to freedom of expression and the right of access to information.

Dissemination of information across the Internet requires an initial supply of information by users of internet services. Every internet user has the ability to upload online content including information about another party (the data subject). Therefore, a conscious decision by an individual to limit the amount of personal information they put online, while prudent, will not necessarily minimise one's online presence or guarantee privacy of such information. Once this information is uploaded, it is available for others online to access and it will be primarily accessed through the medium of a search engine search. Search engines are specifically designed to collect the raw information scattered around the Internet, analyse it and display it in a manner that is convenient for those paying to use their services.

Without search engines, the Internet is practically un-navigable. While the Internet is generally unable to forget information, search engines are the key to accessing its eternal memory. The ubiquitous role of search engines makes it imperative to consider their responsibilities in regard to the personal data they process. However, data protection legal frameworks, even those of global data protection leaders like the European Union (EU), leave the position of search engines largely undefined and uncontrolled.[7]

Where a third party uploads information about an individual online and that information is both factually correct and lawfully published, the data subject's options for having the information removed from the Internet are slight.[8] However, the recent ruling of the Court of Justice of the European Union (CJEU) in *Costeja*[9] changed this. The CJEU looked at the responsibilities of search engines for the personal data that they process and held that the EU's

[7] However, it must be noted that regulation of technology requires flexibility and non-specificity in the law to allow it to keep up with changing developments.
[8] While legal remedies for the removal of lawfully published information online are limited there are alternative means by which one can attempt to supress such information. For example, online reputation management services which have technical means of supressing information online, can be used.
[9] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] OJ 212.

Data Protection Directive (DPD)[10] gives EU citizens the right to directly request that search engines remove links to certain information about them. To warrant a removal, the information concerned must be deemed "inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine" and the data subject's interest in removal must be balanced by the interest of the general public in having access to that information.[11]

This decision effectively makes private companies, with economic interests in managing data, primarily responsible for determining the correct application of EU data protection law. It also allows for people to remove, for all intents and purposes,[12] information that has been lawfully published about them. On analogy with Orwell's view of the future, the ruling gives EU citizens the ability to request elimination of truths published about them and renders search engines the directing brains over the information that goes down the Internet's memory hole into the scattered oblivion of information they will cease to index.

It does not seem desirable to have search engines, that enable individuals to unearth minutely precise personal data about others, unregulated in the way that they process lawfully published information. Similarly, it is not the responsibility of private companies to make complex legal determinations that require the careful balancing of rights, for a mass of fact-dependent complainants. This quandary leads to reflection on broader questions about the position of internet intermediaries in the governance of the Internet and the weighting that should be given to the rights of freedom of expression and access to information versus the need to respect privacy interests. This dissertation will centre on a jurisprudential analysis of the *Costeja* decision and its broader implications.

Chapter I provides a brief overview of the origins and composition of the EU and its national, transnational and supranational law-making processes. It outlines the EU's data protection framework and highlights the key aspects of the DPD, which is currently the most comprehensive supranational legislation

[10] Directive 95/46/EC (DPD) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD) [1995] OJ L 281.
[11] *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja* González, above n 10, at 94.
[12] Viktor Mayer-Schönberger, Professor of Internet Governance at the Oxford Internet Institute, University of Oxford, states "… if you can be deleted from Google's database, i.e. if you carry out a search on yourself and it no longer shows up, it might be in Google's back-up, but if 99% of the population don't have access to it you have effectively been deleted" in Kate Connolly "Right to erasure protects people's freedom to forget the past, says expert" *The Guardian* (online ed, Berlin, 4 April 2014).

on data protection in the EU and the legislation under which *Costeja* was ruled.

Chapter II involves a case analysis of *Costeja*. It evaluates the merits of the different interpretations given by CJEU and the Advocate General on various points of data protection law. This case gave the CJEU the opportunity to examine search engine operator (SEO) liability under the DPD and to determine whether the provisions of the DPD give data subjects the right to have information about them de-indexed from search engine generated search results. The CJEU classified SEOs as data 'controllers' and ordered SEOs to de-index search results, where appropriate.

Chapter III explores the aftermath of the CJEU's ruling. It expands on the CJEU's argument that SEOs are data controllers under the DPD. It highlights the need for greater transparency in the way SEOs are handling requests for removal of links to URLs. It then looks at the potential impact of *Costeja* on the conversation surrounding global internet regulation.

Chapter IV engages with Lawrence Lessig's 'four regulatory constraints' as a model for Internet regulation. It explores key aspects of the proposed General Data Protection Regulation (GDPR) and reflects on the way in which the new regulation will alter the data protection framework in the EU. It discusses the impact that the GDPR will have on SEOs in terms of new compliance requirements for data controllers. It then suggests improvements for the proposed way in which data controllers will be handled under the new regulation and offers up additional and alternative solutions for the improved regulation of personal data processing on the Internet. It will conclude that a combined approach, involving legal and architectural constraints as well as changes to social norms and the market, is the best means for regulating the processing of personal data online.

I: EUROPEAN UNION DATA PROTECTION LAW

The EU finds its origins in the creation of an internal market. Facilitating the integration of a number of different European economic regions was a primary focus for EU lawmakers. Historically, EU lawmakers also placed a high value on protecting the right to privacy and subsequently protection of personal data as a development of that right.[13] In order to explore the area of data protection law in the EU it is important to understand the tension between the dual aims of data protection, namely:[14]

1. Ensuring the free-flow of personal data in the EU, which reflects the "market-making vocation" of data protection law; and
2. The protection of the fundamental rights and freedoms of the individuals whose data is being processed.

The dual objectives of data protection law can be complementary. Ensured privacy in the handling of personal data improves consumer confidence in business and the uniform application of the various rights protections afforded to EU citizens provides greater certainty for businesses with respect to how they conduct themselves when handling personal data.

However, new technologies, like search engines, are difficult to regulate in a way that balances the promotion of the dual data protection aims. Search engines are indispensible tools in the increasingly digitalised economy but they also provide services that can be used in privacy encroaching ways. The first part of this Chapter provides a brief exploration of the origins and composition of the EU. The second part of this Chapter focuses on the national, transnational and supranational legislative and political tools that comprise EU's data protection framework.[15] It then moves on to focus on the key provisions of the DPD relied upon in *Costeja*, a case that tips the balance of the dual aims of data protection in favour of the protection of fundamental rights.

[13] It is important to understand that data protection law is inextricably linked with human rights values. The European legal privacy approach is based on the concepts of "dignity and the fundamental rights and in its early stages in Europe data protection was treated as a subset of the right to privacy.
[14] Orla Lynskey "From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis" in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds) *European Data Protection: Coming of Age* (Springer Dordrecht Heidelberg, New York, 2013) at 60.
[15] SS McCarty-Snead and AT Hilby *Research Guide to European Data Protection Law* (Legal Research Series Paper 1, Berkeley Law Scholarship Repository, 2013) at 13.

A. The Council of Europe and the European Union

The EU and the Council of Europe (CoE) are the two key entities in which the EU member states participate.[16] The CoE was established in 1949 for the purpose of promoting unity among European countries.[17] All EU member states are members of the CoE.[18] The CoE sets the benchmark for human rights, democracy and the rule of law in the European community.[19]

The EU originated from the desire to create a single market in the EU in the years following World War Two[20] and was established under its current name in 1993 by the Maastricht Treaty.[21] In its current formation, the EU is an economic and political partnership between 28 European countries.[22] In forming the EU, legislative sovereignty was relinquished by its member states and a self-sufficient body of law was created that is binding on member states, their citizens and their courts.[23]

The 2007 Memorandum of Understanding (MoU) governs the relationship between the EU and the CoE.[24] The MoU promotes the need for unity in the EU and CoE jurisprudential frameworks that govern the promotion human rights values.

In looking at the origins of the EU and the interactions between the EU and CoE we can clearly see the dual aims of this politico-economic union, namely the creation of a single market and the promotion of fundamental rights in all member states.

[16] McCarty-Snead and Hilby, above n 13, at 4.
[17] Statute of the Council of Europe EUTS 1 (opened for signature 5 May 1949, entered into force 3 August 1949), chapt 1 art 5.
[18] The CoE also has 19 non-EU members which are largely Eastern and Southern European countries.
[19] Committee on Legal Affairs and Human Rights *European Union and Council of Europe human rights agendas: synergies not duplication!* (Parliamentary Assembly, Doc. 13321, 2 October 2013) at 7.
[20] This began with the integration of the European coal and steel communities and the 1957 establishment of the European Economic Community (EEC): "The history of the European Union" European Union <europa.eu>.
[21] Treaty of Maastricht on European Union OJ C 191 (opened for signature 7 February 1992, entered into force 1 November 1992).
[22] "EU member countries" European Union <europa.eu>.
[23] Klaus-Dieter Borchardt *The ABC of European Union law* (Publications Office of the European Union, Luxembourg, 2010) at 115.
[24] "The Council of Europe's Relations with the European Union" Council of Europe <www.coe.int>.

B. European data protection framework

1 OECD Privacy Guidelines

Data protection laws emerged in a piecemeal fashion across European state-level law in the 1970s.[25] The OECD's 1980 privacy guidelines were the first international statement on information privacy. Briefly, the eight data principles in the privacy guidelines specify the need to limit the collection and use of personal data to specified purposes and to maintain transparency in the processing of that data. They also establish that the person who can be identified as the data controller will have the responsibility for complying with these principles.[26] These protection principles are reflected in current EU data protection framework and in data protection legislation globally.

2 Conventions and the Charter of Fundamental Rights

Two conventions of the CoE are supranational sources of EU data protection law: the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR)[27], specifically art 8[28] and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981.[29] The latter convention granted data protection the status of a separate human right. The right to data protection was later enshrined in the Charter of Fundamental Rights of the European Union (ECFR) [30] , which was incorporated into the TEU in 2009 via the Treaty of Lisbon. Article 8 of the ECFR, which relates to the protection of personal data, specifies: [31]

1. Everyone has the right to the protection of his or her own personal data.

[25] The German Hessian Parliament enacted the first information privacy statute in 1970: Daniel J Solove *The digital person: technology and privacy in the information age* (New York University Press, New York, 2004) at 105; from there, other German states and eventually federal German law enacted this type of legislation. The next wave of information privacy legislation was enacted in other European countries: Sweden (1973), Austria (1978), Denmark (1978), France (1978): Murray Laver *Computers and Social Change* (Cambridge University Press, New York, 1980) at 78.

[26] "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" *OECD* < oecd.org>.

[27] Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) CETS 005 (opened for signature 4 November 1950, entered into force 3 September 1953).

[28] Article 8 states that "1.Everyone has the right to respect for his private and family life, his home and his correspondence. 2.There shall be no interference by a public authority with the exercise of this right ...": art 8.

[29] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS 108 (opened for signature 28 January 1981, entered into force 1 October 1985).

[30] Charter of Fundamental Rights of the European Union (ECFR), 2000 OJ C 364/01.

[31] Art 8.

2. Personal data must be processed fairly, for specified purposes and on the basis of consent of the person concerned or some other legitimate basis laid down by law.
3. Everyone has the right of access to data that has been collected concerning him or her and the right to have it revised where necessary.

The intent and effect of EU law is to be understood against the background of the terms of the ECFR, as interpreted by the CJEU.[32] Therefore, any CJEU interpretation of the EU's main legal acts: regulations, directives and decisions[33], will be coloured with human rights jurisprudence, which includes the right to the protection of personal data.

3 Data Protection Directive

This dissertation will focus largely on the DPD, which at present provides the most comprehensive supranational legislation on data protection in the EU.[34] It will also examine the proposed General Data Protection Regulation (GDPR).[35] The GDPR will work to override the DPD over a transitional period.[36] With particular focus on SEO liabilities, Chapter VI of this dissertation will examine ways in which the GDPR may or may not change the data protection landscape.

To understand the significance of this proposed change to the EU data protection framework, it is important to highlight a key difference between directives and regulations:[37]

a. 'regulations' are binding legislative Acts that become law in all member states the moment they come into force, automatically overriding any domestic provisions; whereas
b. 'directives' are not applied uniformly across EU member states in the way that regulations are. Directives require member states

[32] Aidan O'Neill QC "How the CJEU uses the Charter of Fundamental Rights" (3 April 2012) Eutopia Law <eutopialaw.com>.
[33] "European Union legal acts" (29 June 2010) EUR-Lex <eur-lex.europa.eu>.
[34] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201 and Directive 2006/24/EC of the European Parliament and of the Council [2006] OJ L 105 are the two other important pieces of supranational legislation, which are extensions of the DPD.
[35] European Commission text *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)* (COM(2012)0011).
[36] The European Commission has forecasted that the GDPR will be in early 2016 and rolled out in 2017 and 2018: Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers" (June 2015) <www.huntonregulationtracker.com>.
[37] "Regulations, Directives and other acts" European Union <europa.eu>.

> to achieve a certain legislative goal but leave the member state with discretion as to how they would like to achieve that goal.

Once in force, the GDPR will be directly applied in EU member states. Together, the DPD and the GDPR represent the present and proposed objectives for all EU data protection legislation. In drafting the DPD the Commission sought to introduce a "uniform regulatory environment" primarily to address the divergences between member state data protection laws that were making free flow of data across borders difficult for businesses.[38] By ensuring a uniform level of protection for fundamental rights in the context of personal data the EU sought to achieve its market aim.[39] The precise nature of the DPD has been described as difficult to discern: "is it a tool for market integration? Or is it an instrument for the protection of fundamental rights?"[40] The *Costeja* ruling provides some clarification on this point. It signals judicial preference for the latter interpretation. To provide some context and better clarity for the case analysis in Chapter II, a brief introduction to some key sections of the DPD follows:

(i) Objective

Article 1(1) of the DPD states its objects:

> In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

(ii) Definitions

Article 2 provides the following key definitions:

> (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;
>
> (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data,

[38] Lynskey, above n 14 at 61.
[39] At 62.
[40] At 59.

whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction;

...

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...

(iii) Scope

Article 3(1) sets the scope for the DPD:

This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system ...

(iv) Principles relating to data quality

Article 6(1) states that Member States shall provide that personal data must be:

(a) processed fairly and lawfully;

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.

The purpose limitation principle articulated by arts 6(1)(a) and (e) of the DPD implies that once the purpose of the collection and processing has been achieved, the default option is that the personal data should be deleted or rendered anonymous.[41] However, there are exceptions in art 6(1)(b) for "historical, statistical or scientific purposes" and "for the processing of personal data carried out solely for journalistic purposes ... or artistic or literary expression" where it is deemed necessary to reconcile the right to privacy with the rules governing freedom of expression.[42]

(v) Criteria for making data processing legitimate

Article 7 stipulates that Member States shall provide that personal data may be processed only if:

(a) the data subject has unambiguously given his consent; or

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or

(c) processing is necessary for compliance with a legal obligation to which the controller is subject; or

(d) processing is necessary in order to protect the vital interests of the data subject; or

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the

[41] Alessandro Pancani "Searching to be Forgotten: An Investigation of the Effects of the Proposed "Right to be Forgotten and to Erasure" on Search Engines" (Law & Technology Master Thesis, Tilburg Law School, 2013) at 32.
[42] DPD, art 9(1).

interests for fundamental rights and freedoms of the data subject which require protection under art 1(1).

(vi) Right of access

Article 12(1) sets out that: Member States shall guarantee every data subject the right to obtain from the controller:

(b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data ...

2. It shall be for the controller to ensure that paragraph 1 is complied with.

(vii) The data subject's right to object

Article 14 sets out that Member States shall grant the data subject the right:

(a) at least in the cases referred to in arts 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data;

(b) to object, on request and free of charge, to the processing of personal data relating to him which the controller anticipates being processed for the purposes of direct marketing, or to be informed before personal data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

Member States shall take the necessary measures to ensure that data subjects are aware of the existence of the right referred to in the first subparagraph of (b).

Articles 12 and 14 afford data subjects specific reactive rights, these rights have to voluntarily and actively asserted by the data subject in order to be engaged.

II: *COSTEJA*

A. Overview

In this Chapter, it is argued that the CJEU's reasoning in *Costeja* is more persuasive than that of the Advocate General in his Advisory Opinion, particularly so on the key issue of SEO classification under the DPD. However, the CJEU's ruling is brief and it does not elucidate its reasoning for this classification. Chapter III will explore the validity of this classification further.

While *Costeja* did not establish a 'right to be forgotten' for EU citizens, it confirmed the existence of a right under the DPD to have lawfully published information de-indexed by SEOs, where the purposes of processing that information have been satisfied. The major problem with the ruling is that the CJEU foisted decision-making responsibilities about complex jurisprudential issues onto Google, a private company, with only vague guidance.

B. Procedural history of Mr Costeja González's complaints

On 5 March 2010, Mr Costeja González, a Spanish national, lodged complaints with the Agencia Española de Protección de Datos (AEPD) against La Vanguardia Ediciones SL (La Vanguardia), a Catalan newspaper, and against Google Spain and Google Inc.[43] Mr González took issue with two auction notices that La Vanguardia had printed on 19 January and 9 March 1998. [44] The notices detailed the auction of Mr González's house in connection with attachment proceedings for the recovery of social security debts.[45] Both notices were republished at a later date in an electronic version of the newspaper made available on the Internet.

Mr González requested that La Vanguardia be required to remove or alter the publications so that his personal data would no longer appear.[46] He also requested that Google Spain and Google Inc should be required to remove or conceal personal data relating to him so that links to the data would cease to be included in the results generated by the search engine when Mr

[43] *Costeja*, above n 9, at [14].
[44] At [14].
[45] At [14].
[46] At [15].

González's name was searched.[47] Mr González justified these complaints on the basis that his debts and the related attachment proceedings had been resolved many years previously and were no longer of any public relevance and should thus cease to be associated with his name.[48]

On 30 July 2010, the Director of the AEPD rejected the complaint made against La Vanguardia on the basis that the Spanish Ministry of Labour and Social Affairs had ordered the publication of the notices. However, the AEPD upheld the complaints made against Google Spain and Google Inc requesting that Google cease to include links to the La Vanguardia pages in its search results. Google Spain and Google Inc brought separate actions against the decision before the Spanish High Court and the Court joined the two actions.[49]

In March 2012 the Spanish High Court referred a series of questions to the CJEU for a preliminary ruling on the interpretation of the DPD and stayed the proceedings until the points were clarified.[50] In June 2013 Advocate General Niilo Jääskinen delivered an Advisory Opinion to the CJEU. The Advocate General found that SEOs were not liable under the DPD to remove links to data published on third party websites. However, the CJEU, which typically tends to conclude in agreement with the opinions of the EU Advocate Generals, disagreed with this Opinion. [51]

C. Questions referred to the Court of Justice

The questions referred to the CJEU in the Spanish High Court's Order for Reference can be categorised into three main areas of legal issue:

1) the territorial scope of the DPD;
2) the legal position of an SEO, particularly looking at whether an SEO can be categorised as a data 'controller' for the purposes of the DPD; and

[47] *Costeja*, above n 9, at [15].
[48] At [15].
[49] Google Spain and Google Inc from here on will be referred to collectively as 'Google' where it is appropriate to do so.
[50] A preliminary ruling is a procedure exercised before the CJEU; it enables national courts to question the CJEU on the interpretation or validity of European law: "The reference for a preliminary ruling" (15 January 2014) EUR-Lex <eur-lex.europa.eu>.
[51] An Opinion from the Advocate General will propose an outcome for the case. The CJEU is neither bound to follow the course of action proposed by the Advocate General, nor does it need to provide an explanation for why it chose to follow a different course. However, in practice, it is usual for the CJEU to follow an Opinion and the Advocate General's Opinions are therefore often important in elaborating on the judgements of the CJEU which tend to be very brief: Aidan O'Neill QC *EU Law for UK Lawyers* (Hart Publishing Ltd, Oxford (UK), 2011) at 189.

3) the extent to which, if any, the DPD gives EU citizens an effective 'right to be forgotten'[52] on the Internet by way of de-indexing search results concerning them.

Before examining each of these issues, it is necessary to analyse the interpretations and reasoning of both the CJEU and the Advocate General, behind their respective decisions.

The CJEU and the Advocate General had very different interpretive start points. The CJEU relied heavily on the art (1)(1) objective, which states that the DPD exists to 'protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.' The CJEU referred back to the objective on almost every legal issue to steer its analysis in the direction of its goal: setting limits on the ability of the SEOs to provide a "structured overview" of an individual. [53] The CJEU continually asserted that this capability heightens the already palpable threat that the permanence of online information has to a data subject's privacy. The CJEU's analysis also reflects the fact that internet intermediaries are often considered the natural points for control of content online.[54]

The Advocate General focused on the negative impact that subjecting SEOs to data controller liability under the DPD might have on the rights to freedom of expression and access of information as well as the potential chilling effect this could have on the operation of search engine services generally.[55] The differing start points taken by the CJEU and the Advocate General highlight the tension between the different legislative aims of the DPD as described in Chapter I.

[52] This term, although used frequently in popular discussion to capture the ratio of the case, will be used sparingly in this dissertation, as it is misleading. The *Costeja* ruling simply establishes a (non-absolute) right to have results de-indexed by SEOs.
[53] *Costeja*, above n 9, at [37] and [80].
[54] Jonathan Zittrain "A History of Online Gatekeeping, Harvard Journal of Law and Technology" (2006) 19 Harvard JOLT 253 at 254.
[55] Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] OJ 212, Opinion of AG Jääskinen.

(i) Source webpage liability left unquestioned in the order for reference

As a preliminary matter, it is important to note that the CJEU can only advise national courts on questions that they refer to it for preliminary ruling. The AEPD's decision not to pursue the question of La Vanguardia's liability put the question of source webpage liability under the DPD out of the scope of the CJEU. The AEPD decided that La Vanguardia's auction notices could remain online, untouched, on the basis that at the time of publication, a government agency lawfully instructed their printing. In a seemingly contradictory fashion, the AEPD upheld the complaint against Google on the basis that the purpose of the advertisement had been fulfilled many years prior and the information was no longer relevant. The fact that the AEPD chose to allow the information that created the initial harm to remain online can perhaps be considered an act of compromise. Pursuit of La Vanguardia would potentially have lead to complete removal of the article, which would be tantamount to censorship, potentially an interference with the freedom of the press[56] and for that matter, history. However, the reasoning the AEPD used to reach this compromise was contradictory. Placing the full burden of the complaint on the SEOs creates a feeling of uncertainty about the correctness of the CJEU decision.[57] It would have been beneficial to have a statement from the CJEU on the question of source webpage liability under the DPD.

Despite not being within the scope of questions referred for preliminary ruling, the Advocate General looked at the role and liability of source web page publishers under the DPD.[58] He relied on the CJEU's findings in *Lindqvist*[59] that "the act of referring on an internet page, to various persons and identifying them by name or by other means ... constitutes 'the processing of personal data wholly or partly by automatic means' within the meaning of art 3(1)..." of the DPD. [60]

The Advocate General held that it followed from the CJEU's findings in *Lindqvist* that those who publish personal data on source web pages, which is very much an intentional act, are controllers of processing of personal data within the meaning of the DPD.[61] He found that the publisher should be identified as the true controller of processing of personal data and that any

[56] Though the auction notices were not news stories, but essentially an advertisement.
[57] Rigo Wenning "The ECJ is right, the result is wrong" (16 May 2014) Internet Law: Online Legal Affairs 2.0 <www.internet-law.de>.
[58] *Costeja*, AG Jääskinen, above n 55, at [39].
[59] Case C-101/01 *Lindqvist* [2003] ECR I-12971.
[60] At [19].
[61] *Costeja*, AG Jääskinen, above n 55, at [40].

publisher also has the means of fulfilling his or her obligations in this respect.[62] He concluded: "this channeling of legal liability through the person who publishes the content on the source web page is consistent with the established principles of publisher liability in the context of traditional media." [63] By this reasoning, the Advocate General would identify La Vanguardia as the controller of processing of personal data within the meaning of the DPD.

1 Territorial scope

The territorial reach of the DPD is established in art 4 entitled 'National law applicable', which provides that:

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

> (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State;

(i) Is Google Spain an 'establishment'?

Data controller liability under the DPD depends not on the physical location of its data processing business but on the data controller's place of establishment. [64] In *Costeja*, it did not matter that Google is a California-based company. Nor was it disputed that Google Spain is an establishment of Google.

(ii) Is processing being carried out 'in the context of activities of the establishment'?

The Advocate General recommended that assessment of the territorial applicability of the DPD be determined by way of analysing Google's business model.[65] The Google business model is premised on the sale of keyword advertising, a system that matches a user's search query with bespoke

[62] The Advocate General pointed to the fact that the publisher has the possibility to include in his web pages, exclusion codes restricting indexing and archiving of the page and thereby enhancing protection for personal data and in extreme cases, the publisher can withdraw the page from the host server, republish it without the objectionable personal data and require updating of the page in the cache memories of search engines: at [42] – [43].
[63] At [43].
[64] An establishment on the territory of a member state implies the effective and real exercise of activity through stable arrangements, the legal form of the establishment is not a determining factor: DPD, recital 19.
[65] *Costeja*, AG Jääskinen, above n 55, at [64].

advertisements according to keywords and categories searched.[66] By the Advocate General's reasoning, keyword advertising renders data processing the economic "raison d'être" for the provision of a free information location tool.[67]

The CJEU reached the same conclusion but used a different approach. The CJEU focussed primarily on the objective of and recitals 18 to 20 of the DPD.[68] The CJEU considered these to be strong indicators that the DPD should be given a broad territorial scope so as to prevent circumvention of its intended protections.[69] The CJEU did however find, in agreement with the Advocate General, that the keyword advertising business model confirmed that the processing of data by Google is carried out 'in the context of the activities' of that establishment.[70] The Article 29 Working Party (A29WP)[71], in terms of the use of cookies, has also articulated this assessment of behavioural advertising.[72]

2 Legal position of search engine operators

In order to allocate responsibility under the DPD, the controller of data processing[73] must be identified. Article 2(d) of the DPD defines a 'controller' as:

> ... the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...

(ii) The Advocate General's Opinion on SEOs being classified as data 'controllers'

[66] Google's targeting advertisement system carefully matches a user's search query with closely related advertisements that are based on key words and categories searched: Kimberley Vogel "Google's Targeted Keyword Ad Program Shows Strong Momentum with Advertisers" News from Google <googlepress.blogspot.co.nz>.
[67] *Costeja*, AG Jääskinen, above n 55, at [64].
[68] *Costeja*, above n 9, at [54].
[69] David Lindsay "The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling" (2014) 6 JML 159 at 164.
[70] *Costeja*, above n 55, at [57].
[71] The Article 29 Working Party (A29WP) was set up under arts 15 and 30 of the DPD in order to provide expert advice and promote uniform application of the DPD as well as advise the European Commission on anything affecting the right to protection of personal data: "Article 29 Working Party" European Data Protection Supervisor <secure.edps.europa.eu>.
[72] A29WP *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010) at 11.
[73] SEOs, by searching 'automatically', 'constantly' and 'systematically' for information published on the internet 'collect' data. Within the frameworks of indexing programmes SEOs 'record' and 'organise' then 'store' it on servers and 'disclose' the processed information to their users: *Costeja*, above n 9, at [28].

The Advocate General followed the A29WP 2008 Opinion on search engines[74] and its 2010 Opinion on the concepts of 'controller' and 'processer.' [75] The 2008 opinion the A29WP sought to "strike a balance between the legitimate business needs of the search engine providers and the protection of the personal data of internet users."[76] The A29WP drew a distinction between SEOs when they are performing a passive intermediary function and where they go beyond this by, for example, providing caching functionality or storing web content on their servers, in which case SEOs may be considered data controllers. The A29WP concluded that when an SEO is acting purely as an intermediary provider of access to data they could not be considered controllers.[77]

In its 2010 Opinion, the A29WP found that in order to identify the controller, one must examine the "purpose for and drive" behind the data processing.[78] The Advocate General emphasised that the purpose of the DPD is to allocate responsibility to the locus of control. He identified the controller as being the party who *intentionally* processes data as personal data in a "semantically relevant way".[79] The Advocate General interpreted the phrasing of art 2(d) as requiring that the controller is "aware of the existence of a defined category of information amounting to personal data." [80]

On this point, the Advocate General identified the broader legal principle that "automated, technical and passive relationships to electronically stored or transmitted content did not create control or liability over it."[81] The Advocate General described how the technical and automated process of storing data on the cache memory simply produces a mirror image of the text data of webpages crawled by the Googlebot.[82] He found that, only where the SEO did not comply with exclusion codes, such as the robots.txt file or

[74] A29WP, *Opinion 1/2008 on data protection issues relating to search engines* (WP 140, 4 April 2008).
[75] A29WP, *Opinion 1/2010 on the concepts of 'controller' and 'processor'* (WP 169, 16 February 2010).
[76] A29WP, *Opinion 1/2008 on data protection issues relating to search engines,* above n 74, at 3.
[77] At 14.
[78] A29WP, *Opinion 1/2010 on the concepts of 'controller' and 'processor',* above n 75, at 8.
[79] *Costeja*, AG Jääskinen, above n 55, at [83].
[80] At [83].
[81] *Costeja*, AG Jääskinen, above n 55, at [87].
[82] "Google's search engines crawler function called 'Googlebot' crawls on the Internet constantly and systematically, advancing from one source web page to another on the basis of hyperlinks between the pages, requesting the visited sites to send it a copy of the visited page. The copies of the source web pages are analysed by Google's indexing function. Sign strings (keywords, search terms) found on the pages are recorded in the index of the search engine. Google's elaborate search algorithm also assesses the relevance of the search results. Combinations of keywords & URL addresses form the index of the search engine. The searches initiated by users are executed within the (pre-formed) index": "Googlebot" Search Console Help <support.google.com>.

NoIndex/NoArchive tags, could the SEO can be held to be a controller of processing personal data. Non-compliance with these kinds of codes would demonstrate that the provider of the content, namely the SEO, has exerted sufficient intentional control to be responsible for the personal data processed and could therefore be appropriately deemed a data controller under art 2(d).[83]

(iii) The CJEU's Opinion on SEOs being classified as data 'controllers'

In contrast with the Advocate General, the CJEU found it irrelevant that search engines use a uniform processing method in respect of most types of information and does not distinguish between non-personal and personal data.[84] Therefore, the CJEU also found the issue of (non) compliance with exclusion codes extraneous to the question of control.[85] The CJEU again focused its interpretation on the "decisive role" that SEOs play in dissemination of information on the Internet.[86] The CJEU described the way that search engines organise and aggregate information, a function which can be used to create a "structured overview"[87] of an individual, as liable to affect significantly the "fundamental rights to privacy and protection of personal data."[88] The CJEU determined that in order to give full effect to the objective of the DPD the conclusion that SEOs are data controllers within the meaning of art 2(d) had to be reached. This line of reasoning rejects Google's general adamancy that their systems are automatically programmed, rendering them passive online players. When engaging in activities like ad-targeting, Google has issued 'reassuring' statements like: "Ad targeting in Gmail is fully automated" and "no humans read your email in order to show you advertisements or related information."[89] However, it does not seem logically sound to forever allow Google to excuse itself from liability on the basis that it is only a cache when it has, in fact, "diligently programmed" and "fully controls" the activities of its crawlers.[90] This idea will be explored further in Chapter III.

[83] Lindsay, above n 69, at 167.
[84] *Costeja*, above n 55, at [28].
[85] The CJEU considered that the only possible relevance of exclusion codes is when a publisher fails to use them this may create a scenario of joint liability between publishers and SEOs on the basis that by not including them publishers have deemed content appropriate for processing: at [40].
[86] At [36].
[87] At [37].
[88] At [38].
[89] "Ads in Gmail" Google <support.google.com>.
[90] Wenning above n 57.

3 The 'right to be forgotten'

Although this case focuses on obligations owed by search engines under the DPD, its broader implication is whether a 'right to be forgotten' can be found within its provisions. Once a controller is allocated responsibility under the DPD, the scope of the obligations owed by the controller must be assessed. [91]

Article 12 of the DPD provides that member states are to guarantee every data subject the right to obtain from the controller:

> ...
>
> (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data;
>
> ...

It is important to note that this right arises only on occasions where data processing is contrary to the DPD. However, the DPD generally requires controller compliance with the data quality principles set out in art 6 and the criteria for making data processing legitimate in art 7.

Article 6(1)(e) requires member states to include an obligation for personal data to be:

> kept in a form, which permits identification of data subjects, for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

To comply with this obligation, data may be dealt with in various ways, such as by deletion or through anonymisation.

Article 14(a) entitled 'The data subject's right to object', provides that member states shall grant the data subject the right:

> ... to object at any time on compelling legitimate grounds... to the processing of data relating to him, save where otherwise provided by national legislation...

[91] Lindsay, above n 69, at 168.

The controller must stop the processing of the data in question where the data subject's objection is justified. As with art 12(b), this provision is subject to several limitations. Of particular importance, the onus lies with the data subject to point to 'compelling legitimate grounds' to object to the data processing. Further, national legislatures can place limits on this right by derogating from it in other national legislation.

(i) The Advocate General on whether the DPD incorporates a 'right to be forgotten'

The Advocate General explored the question of whether a 'right to be forgotten' can be founded on art 12(b) and art 14(a) of the DPD in case he was wrong about other points. In relation to art 14(a), the Advocate General framed Mr González's request as a "subjective preference" which did not amount to a "compelling legitimate ground" for removal.[92] Furthermore, the Advocate General considered that the phrasing 'in particular' in art 12(b) confines the applicability of any such right to instances where the data in question is incomplete or inaccurate.[93] Mr González's complaint did not assert that the data in question was either of those. The Advocate General then went on to suggest that no search engine index or its cache could be regarded as incomplete or inaccurate by its very nature to copy information exactly.[94]

However, as was noted by the CJEU, 'in particular' can be interpreted as including other instances and the two mentioned can be construed as particular instances. Furthermore, art 6(1)(d) requires that personal data be 'accurate and, where necessary, kept up to date' and art 6(1)(e) permits identification of data subjects for 'no longer than is necessary' for the purposes for which the data are collected and processed. The Advocate General's analysis overlooks the purpose limitation principle in art 6, which offers passively engaged, automatic protection for data subjects.[95] The wording of art 6 implies that once the purpose of the collection and processing has been achieved, the default option is to delete the personal data or render it anonymous.[96]

(ii) The Advocate General's analysis in light of the ECFR

[92] *Costeja*, AG Jääskinen, above n 55, at [108].
[93] *Costeja*, AG Jääskinen, above n 55, at [104].
[94] At [105].
[95] Jef Ausloos "The Right to be Forgotten – It's about time, or is it?" (24 January 2004) Tech, Policy and Society <jefausloos.wordpress.com>.
[96] Pancani, above n 41, at 32.

As noted in Chapter I, any interpretation of EU law expressly requires consideration of the terms of the ECFR. The Advocate General emphasised the need to consider art 11 of the ECFR, which enshrines the right to freedom of expression and protects the right of Internet users to seek and receive information on the Internet.[97]

The Advocate General emphasised that the use of the indispensible services provided by SEOs, is "one of the most important ways" of exercising the art 11 right.[98] The Advocate General further noted that incorporated in the art 11 right is a protection afforded to publishers to make their content available. Ordering SEOs to remove links to content can be seen to be interfering with a publisher's right to disseminate publications.[99] However, it must be noted that the classification of publishers of source webpages as data controllers would have the same limiting effect on a data publisher's right to disseminate publication and could potentially result in the complete removal of the publication online, which has more serious consequences in terms of censorship. SEOs are one step removed from that, which would enable commentators to utilise a freedom of speech argument. Any such position would be more easily shown by the assertion that allowing the original source to publish and attributing data controller liability to the search engine might better enhance this right.

The Advocate General stressed that:[100]

> ... the fundamental right to information merits particular protection in EU law, especially in view of the ever-growing tendency of authoritarian regimes to limit access to the Internet or to censure content made accessible by it.

The Advocate General gave due regard to Google's freedom to conduct a business, a right enshrined by art 16 of the ECFR. The Advocate General cited the commentary in *Scarlet Extended*[101] that "... the freedom to conduct a business [is a right] enjoyed by operators such as ISPs pursuant to Article 16 of the Charter."[102] The Advocate General used this commentary to posit that the cost of implementation of an interpretation of arts 12 and 14 that gives a

[97] *Costeja*, AG Jääskinen, above n 55, at [121].
[98] At [131].
[99] *Costeja*, AG Jääskinen, above n 55, at [134].
[100] At [121]; however there is a counter point that authoritarian regimes, like the totalitarian state of Nazi Germany, have actually used comprehensive population registries to single out and persecute certain groups in society: Viktor Mayer-Schönberger *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, New Jersey, 2009) at 156.
[101] Case C-70/10 *Scarlet Extended* [2011] ECR I-11959.
[102] At [46].

data subject the right to request removal of links would be significant and would result in huge procedural challenges for compliance. However, he did note that this would of course depend on the eventual mechanism that would be established in order to effect compliance, an issue that will be explored in Chapter VI. A flaw in the Advocate General's argument here is that the right of freedom to conduct a business is a human right and not the right of a legal person like the multinational corporation Google.

Overall, the Advocate General found that the DPD did not incorporate a right to be forgotten which would entitle a data subject to demand restriction or termination of the dissemination of personal data.

(iii) CJEU on whether the DPD incorporates a 'right to be forgotten'

In contrast, the CJEU remained consistent in the way it had interpreted the DPD throughout the case. The CJEU examined the application of the rights conferred by these substantive provisions in light of the DPD's objective and also referred specifically to recital 10, which states that the object of EU data protection law is to ensure a "high level of protection of privacy."[103]

Contrary to the Advocate General's approach with regard to art 12(b) the CJEU found that particular reference to 'inaccurate and incomplete' simply amounts to the provision of examples and is not exhaustive.[104] The CJEU considered that the right to rectification, erasure, or blocking could arise from the SEOs non-compliance with any of the DPD provisions. It interpreted art 6(1) as requiring that the controller take every reasonable step to ensure that data complies with the principles of data quality.[105]

(iv) The CJEU's analysis in light of the ECFR

The CJEU noted that assessment of compelling legitimate grounds, as required by art 12(b), requires a careful balancing of competing interests and rights and that this balancing must take into consideration the "significance of the data subject's rights arising from Articles 7 and 8" of the ECFR.[106] The CJEU found that these rights override, as a rule, the economic interest of the

[103] *Costeja*, above n 9, at [66].
[104] At [70].
[105] At [72].
[106] At [74].

SEO, as well as the interest of the general public to access that information.[107]

The CJEU found that, because the functions of SEOs constitute a "more significant interference" with the data subjects right to privacy than the source publication itself, there might be instances where the balance of rights and interests weighs against removal of personal data but where there an SEO may still be required to restrict access to that material. [108]

The CJEU stated that the balancing exercise involves taking into account all of the circumstances surrounding the data subject's particular situation.[109] The CJEU interpreted art 7(f) as allowing the processing of personal data, where it is necessary for the legitimate interests of the controller (or third parties), unless the fundamental rights and freedoms of data subjects override these. Here, the CJEU made a very systemic argument regarding the legal nature of the DPD.[110] It worked backward from the premise that processing personal data is prohibited in Europe unless there is either a legal ground or permission by the data subject to process the data. In *Costeja*, Google did not have either.[111]

The CJEU's ruling

Overall, the CJEU ruled that SEOs are data controllers within the meaning of the DPD. To comply with the DPD, the CJEU found that SEOs must stop linking results to information, where that information is held to be "inadequate, irrelevant or no longer relevant, or excessive in relation to those purposes and in the light of the time that has elapsed." This is to be balanced with the public interest in having access to that information, particularly because of the role played by the data subject in public life. [112] This decision was unable to be appealed because the CJEU is the EU's highest court.

[107] At [97].
[108] *Costeja*, above n 9, at [87].
[109] At [76].
[110] Wenning, above n 57.
[111] Wenning, above n 57.
[112] *Costeja*, above 9, at [93].

III: AFTERMATH OF THE *COSTEJA* DECISION

The *Costeja* ruling attracted interest from a broad variety of parties:

> Marc Rotenburg, the president of the Electronic Privacy Information Center described the decision as "forward looking" and commended the CJEU for effectively telling Google: "[i]f you are going to be in the business of search, you are going to take on some privacy obligations."[113]
>
> Jules Polonetsky, the executive director of the Future of Privacy Forum stated that the decision is one "[r]equiring Google to be a court of philosopher kings," which "shows a real lack of understanding about how this will play out in reality." [114]

Though the above statements seem irreconcilable, each party has acutely raised important considerations which are the each the product of different vested interests. Analysing the *Costeja* ruling through each of these lenses provides great insight.

There are two major competing legal principles at play in the commentary around the ruling. The technology industry advocates freedom of access to information and the importance of free speech, whereas privacy rights and data protection advocates have rallied around the competing idea of the right to be forgotten. [115]

As noted by the Advocate General, search engines are the key means of accessing information on the Internet; a service that is hugely important as society progresses further into the digital age. Conversely, their search capabilities threaten the right to privacy. This suggests that SEOs should take on some responsibility for the data that they process. However, giving a private company like Google, with an economic interest in streamlining the removals process, the responsibility of making determinatons on removals, does not appear to be a desirable solution when it creates the possibility of illegitimate censorship.

---

[113] Marc Rotenburg, the president of the Electronic Privacy Information Center, in Washington, D.C.: Jeffrey Toobin "The Solace of Oblivion" *The New Yorker* (online ed, New York, 29 September 2014).
[114] Jules Polonetsky, the executive director of the Future of Privacy Forum, a think tank in Washington: Toobin, above n 113.
[115] Amir Mizroch "What Is the 'Right to Be Forgotten?'" *Wall Street Journal* (online ed, London, 13 May 2014).

This Chapter begins by building on the CJEU's interpretation in *Costeja*; that SEOs are data controllers. Next, the mechanisms that have been implemented by search engines in order to effect compliance with the ruling will be detailed along with discussion of the key issues surrounding implementation of these mechanisms. Finally, the chapter will consider the potential international reach of the decision.

A. Confirming why search engine operators are data 'controllers'

The decision signals a clear rejection of the 'card catalogue' metaphor that has so often been used to describe the role of SEOs as passive intermediaries in the modern information economy. If we recall, art 2(d) of the DPD defines the 'controller' as:

> ... the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data ...

SEOs fit within this definition by virtue of their algorithmic determinations on the processes and means of how data is processed and displayed. This claim is bolstered by an examination of the Google search result ranking system; noting the way Google has been classified in cases involving defamation and by looking at the profit-driven Google 'Adwords' advertising system.

1 Results of search are significant

'Googling' has become the proprietary eponym for searching on the Internet. It is most pervasive search engine in the EU with a 90% market share.[116] It is in full control of the digital programming of this ranking system.

Google's monopoly on the search engine market in the EU makes it the focus for this part of the analysis. Although the data controller classification will apply to all SEOs, the evidence that SEOs do not perform a passive cataloguing role is most pronounced in the case of Google.

Google engages in a three-step process in order to generate search results: crawl, analyse and respond. The response mechanism involves identifying webpages that score most highly for the query and then displaying those

[116] Emanuele Tarantino "A note on vertical search engines' foreclosure" Joseph E. Harrington Jr and Yannis Katsoulacos (eds) *Recent Advances in the Analysis of Competition Policy and Regulation* (Edward Elgar Publishing, Cheltenham (UK), 2012) 163 at 166.

webpages in order of relevance. These indexes are manifested in the form of hyperlinks and snippets, formats that exist purely for the facilitation of access to the material at the source webpage.

The collective results of a Google search are generally more important than the information on any individual website.[117] Studies have found that from an average search, results listed by Google on the first page generate 92% of all the traffic from anyone making that search.[118]

In light of this statistic, proprietary technologies like those offered by Reputation.com have been developed to create "a more balanced profile" for individuals online.[119] These technologies manipulate the results of Google's search algorithm by seeding additional information on the web to cause links, that the individuals using the service consider undesirable, to appear much lower in a Google search.[120] Demand for these sorts of technologies highlights the prominence of the Google search function in the process of unearthing information online.

2 Search engine operator liability in defamation

The liability of SEOs for linking to defamatory or illegal content on source webpages is an area of law that has been traversed far more than SEO liability for linking legal content.

It is understood that, in a defamation suit, the words complained of must be defamatory in nature. This dissertation involves an examination of SEO liability where the information complained of is lawfully online. However, it is useful to examine the way in which search engine functionality has led to its classification as a joint-publisher in the linking of defamatory content.

In the Australian case *Trkulja v Google Inc*, Beach J concluded that search engines, while operating in an automated way, did so precisely as was programmed by those who owned them.[121] Beach J highlighted the fact that a conscious intention to publish was not a requirement at common law.[122] The Court in that case determined that Google's algorithmic engineers perform an

[117] Toobin, above n 113.
[118] When moving from page one to two, the traffic dropped by 95%, and by 78% and 58% for the subsequent pages: "The Value of Google Result Positioning (7 June 2013) Chitka Online Advertising Network <chitika.com>.
[119] "Combat Negative Search Results With Reputation-Defender ®" Reputation.com <www.reputation.com>.
[120] Peter Sondergaard "Wake up to the Algorithm Economy" (5 August 2015) Gartner <www.gartner.com>.
[121] *Trkulja v Google Inc LLC & Anor* (No 5) [2012] VSC 533 at [27] per Beach J.
[122] At [28] per Beach J.

editorial function stating: “Google…intended to publish the material that its automated systems produced because that was what they were designed to do.” [123]

Search engine processing of personal data is the same regardless of whether the source webpage that it is linked to contains defamatory statements or lawfully published information. Leading defamation cases suggest that awareness of the data’s nature data is superfluous to establishing whether SEOs have an active role in the processing of that data. The Advocate General’s interpretation of the DPD definition of ‘controller,’ namely the person or entity that is processing the data as personal data in a semantically relevant way not as mere computer code, does not hold because that computer code that was systematically and intentionally programmed by Google.[124]

3 Profit-driven algorithmic programming

Google’s online advertising mechanism ‘Adwords’ is the driving force behind the Google indexing system. This is the aspect of Google that really puts the lie to the simple conduit characterisation. Google makes its money by selling advertising that is specifically targeted. Targeting is achieved by directing people to precisely the results that they most want to see and use. Without traffic, Google has no business. Google built an algorithm to learn about users over time and then to tune results to each user. The more refined the data, the more expensive the advertising slot.

It is clear that Google’s algorithmists are in full control of how information is processed, ranked and displayed. It holds true that “[s]earch engines are not disembodied neutral tools but reflect the editorial control of their designers,”[125] However, being classified as such in *Costeja* lead to Google taking on a jurisprudential role under very vague guidelines. This requires further consideration.

B. Mechanisms For Achieving Compliance

The decision to place Google in the position of first point of contact in the de-indexing decision making process has lead to major concern over the issues of procedural fairness and the application of the rule of law.

[123] At [18] per Beach J.
[124] *Costeja*, AG Jääskinen, above n 55, at [83].
[125] Laura Denardis “The Emerging Field of Internet Governance” in William H. Dutton *The Oxford Handbook of Internet Studies* (Oxford University Press, 2013) at 24.

1 Removal request forms

Peter Fleischer, Google's Global Privacy Council, said that devising an implementation strategy was complex, largely because of the CJEU's vagueness.[126] To give effect to the decision, Google created an online request form that allows EU citizens to ask for personal data to be removed from online search results.[127]

To make a request, an individual must be able to verify their identification. The request form asks the individual to list specific URLs that they take issue with and provide an explanation about why they consider the information on the webpage linked by the URL 'irrelevant, out-dated or otherwise objectionable'.[128]

To process requests Google created a removals team. A panel of lawyers, engineers and paralegals reviews the decisions made by this team. Senior lawyers and engineers deal with the removals perceived as being more difficult.[129] In making the determinations, the removals team must balance the individual's interest in having the link removed, with the "interest of the public in having that information, an interest which may vary according to the role played by the data subject in public life."[130] Google cites financial scams, professional malpractice and criminal convictions, as examples of information that public will prima facie have an interest in.[131]

A form similar to the one offered by Google has been made available on both *Yahoo!* and Bing. The *Yahoo!* request form mirrors Google's almost exactly, whereas, the Bing request form is far more onerous on the filing applicant. The latter asks the applicant to detail whether or not they are a public figure ("politician, celebrity, etc."), whether or not they currently have, or expect to have a role in the local community or more broadly, any role that involves leadership, trust or safety ("teacher, clergy, community leader, police, doctor,

[126] Peter Fleischer, at the IAPP Europe Data Proetction Congress in Brussels, stated that the CJEU gave "vague" guidance on how to implement its decision: Loek Essers "This is how Google handles 'right to be forgotten' requests" (19 November 2014) Computer World <www.computerworld.com>.
[127] "Search removal request under data protection law in Europe" Google Legal Help < support.google.com>.
[128] "Search removal request under data protection law in Europe", above n 127.
[129] Fleisher and Schechner, above n 130, at 17.
[130] Sandy Davidson "Right to be Forgotten" (11 June 2014) Jurist <jurist.org>.
[131] "FAQ: How are you implementing the recent Court of Justice of the European Union (CJEU) decision on the right to be forgotten?" Google Privacy & Terms < www.google.se>.

etc."). Furthermore, it asks for a "more detailed substantiation" requiring precise reasons for removal of search results.[132]

(i) Notification of removals

Google of its own initiative includes the notice: "results may have been removed under data protection law in Europe", at the bottom of the search results page whenever a search can be algorithmically identified as a 'name search', not only when the name has been subject to a removal.[133] There is no legal requirement that SEOs must make it apparent to other search engine users that the list of results is not complete as a consequence of a removal approval.[134]

(ii) Transparency report

For the sake of transparency, Google has launched a page detailing statistics and other factual information on submitted requests.[135] The data is updated regularly. As of 21 September 2015, Google has received 318,269 removal requests regarding a total number of 1,126,518 URLs. Across all 28 member states, 41.6 per cent of the URLs that have been made the subject of a removal request have been de-linked and 58.4 per cent have been rejected. Google also details the kinds of removal requests that it has encountered, providing brief details about which ones succeeded and which ones that didn't. Examples of successful requests for removal include:

1. An article about a German teacher's decade old conviction for a minor crime.
2. A reposted self-published image of an Italian woman.
3. An article about an individual in Belgium who had been convicted of a serious crime in the last five years but whose conviction was quashed on appeal.

Examples of unsuccessful requests for removal included:

[132] "Request to Block Bing Search Results In Europe" <www.bing.com>.
[133] Because this notice does not discriminate between name results and name results for which removal of links has occured, it does not provide any indication that a searcher should go onto the .com version of the Google site.
[134] Notification of removal would only be appropriate if information is presented in such a way that the user cannot determine that the particular individual has asked for de-linking of results concerning them.
[135] "European privacy requests for search removals" Google Transparency Report < www.google.com>.

1. An article that reported on the sentence and banishment from the church of a French priest convicted for possession of child abuse imagery.
2. A recently published article discussing the decades old criminal conviction of a high-ranking public official from Hungary.
3. Articles about a prominent businessman's lawsuit with a newspaper.

It is important to note that, where a request for removal does not succeed, the individual may appeal to their local Data Protection Authority (DPA). Source webpages have the same rights as the data subject to appeal to the data protection authority regarding the search engine's decision to de-index its information. This means that the DPAs are final arbiters of the decision. The DPA has the ability to overturn the SEO's decision. However, low appeal rates have been cited, around one per cent of requesters, as evidence of the balancing test being conducted appropriately by Google.[136]

Information on appeal rates does not provide clear evidence that the balancing is being conducted properly. An open letter to Google from 80 well-regarded academics addressed the issue of transparency. Emphasised in the letter is the fact that only incidental challenges to the information being de-listed can be made because there has no formal involvement of original sources or public representatives in Google's decision-making process.[137]

Though the CJEU was silent on the issue in its ruling, the A29WP guidelines recommend that search engines should not, as general practice, inform the 'webmasters' of the delisting.[138] The A29WP does recommend, however, that in difficult cases, where it is necessary to get a "fuller understanding about the circumstances of the case" it may be legitimate for SEOs to contact the original publishers.[139] This approach is likely attributable to concerns that notifying source webpages may have a potential Streisand effect.[140]

Despite the A29WP recommendations, Google has been notifying website administrators when a link to one of their websites is removed on the basis that these removals were not the subject of defamation, the removals instead

[136] Ellen P. Goodman "Dear Google: open letter from 80 Internet Scholars: Release RTBF Compliance Data" Medium < medium.com>.
[137] Goodman, above n 138.
[138] A29WP *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González* C-131/12 (WP 225, 26 November 2014) at 3.
[139] At 3.
[140] The 'Streisand effect' refers to the situation where, despite or even as a result of, attempts to hide or censor information, the information becomes more public: "Streisand Effect" technopeadia <www.techopedia.com>.

relate to "valid and legal content."[141] However, Google does not provide website adminstrators with information about why the content has been removed, which renders this practice of informing for reasons of transparency, void of real transparency. Despite recommending that SEOs refrain from informing webmasters, to achieve transparency the A29WP stressed the need for "search engines to provide the de-listing criteria they use, and to make more detailed statistics available."[142] While it must be recognised that there is an obvious tension between transparency and the protection of privacy, the jurisprudence involved in Google's approach is being "built in the dark".[143]

2 Highlighting the need for greater transparency

Google on its FAQ page responds to the question of how it is implementing the *Costeja* decision. It asserts, "...as a private organisation, we may not be in a good position to decide on your case."[144] It is problematic that the vagueness and lack of prescriptiveness in the CJEU's ruling creates a situation where private company with an economic interest in streamlining the removals process is the first point of contact for determining the correct application of European data protection law.

Further, the practical difficulty of implementing the CJEU's ruling must be appreciated. Implementation involves careful balancing of a host of complex jurisprudential principles to a mass of fact-dependent complaints.

There have been a number of accusations made which suggest that Google has been tactically implementing the *Costeja* decision. Of notable mention is the accusation that Google are over-interpreting the ruling to create moral panic about forced censorship.[145]

Ryan Heath, spokesman for the European Commission's vice-president Neelie Kroes, accused Google of misinterpreting the ruling by deleting links to apparently harmless news articles and to articles that are clearly in the public interest, in a bid to whip up anger about censorship.[146] Alexander Hanff, chief

[141] Goodman, above n 138.
[142] A29WP *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González*, above n 140, at 3.
[143] Goodman, above n 138.
[144] "FAQ: How are you implementing the recent Court of Justice of the European Union (CJEU) decision on the right to be forgotten?", above n 133.
[145] Alexander Hanff, chief executive of Think Privacy group accused Google of removing links unnecessarily: Jonathan Owen "Is Google sabotaging the 'right to be forgotten'?" (4 July 2014) New Zealand Herald <www.nzherald.co.nz>.
[146] Robert Peston "Why has Google cast me into oblivion?" (2 July 2014) BBC News <www.bbc.com>.

executive of the Think Privacy Group, accused Google of removing links unnecessarily "in order to apply political pressure into having the ruling challenged."[147] For example, Google's decision to remove a BBC article about ex Merrill Lynch boss Stanley O'Neal, one of those blamed for helping cause the global financial crisis, was extremely controversial.[148] The author of the article removed, Robert Peston, asserted that:

> Most people would argue that it is highly relevant for the track record, good or bad, of a business leader to remain on the public record - especially someone widely seen as having played an important role in the worst financial crisis in living memory.

The trouble is that it was "almost certain" that the deletion in this instance came as a result of a request made by one of the readers commenting in the thread beneath the article who presumably wanted to be disassociated with the comment. This illustrates the complexity of Google's task in effecting compliance.[149] Whether or not Google over-interpreted the ruling with regard to O'Neal remains to be seen.

Of more importance is that this is empirical evidence demonstrating that publications of legitimate expression can become collateral damage when private companies are placed in the position of making determinations on the balance of rights. This issue is exacerbated by the fact that "[b]eyond anecdote, we know very little about what kind and quantity of information is being delisted from search results, what sources are being delisted and on what scale..."[150]

3 Territorial reach of removals

The lack of prescriptiveness in the ruling gave Google a great amount of discretion on the territorial breadth of removal. Google decided that URLs approved for removal would be de-indexed from the results of searches, not only on national versions of Google in the 28 EU member states but also from Google's domains in Iceland, Liechtenstein, Norway and Switzerland; countries belonging to the European Free Trade Association (EFTA).[151] It is significant that Google determined the territorial breadth of this decision's

[147] Owen, above n 147.
[148] Peston, above n 148.
[149] Toobin, above n 113.
[150] Goodman, above n 138.
[151] Byung-Cheol Kim and Jin Yeub Kim "The Economics of the Right to be Forgotten" (16 March 2015) <econ.msu.edu>.

reach as it allowed Google to set a benchmark for other companies in terms of public expectation.

C. *Costeja's* international effects

While the CJEU only required that Google de-index information from subsidiary search engines within the EU, Google's current approach to implementation arguably undermines the effectiveness of the CJEU's ruling.[152] The A29WP recommended that de-listing should be effective on all relevant domains, including Google.com.[153] However, the A29WP do not address the issue of extra-territorial effect as a result of expansive de-indexing.

1 Principle of territoriality

The principle of territoriality is fundamental to jurisdictional questions in public international law.[154] The approach of 'territorial zoning' is already largely a reality in the context of the Internet.[155] Many multinational corporations, like Google, already have country specific websites with censorship policies that are compliant with the regulatory requirements of particular states.[156] To ask an SEO to remove links to information on a global scale could potentially lead to a situation where only the content tolerated by the most restrictive regime would remain online.[157] This kind of argument suggests that the geographical borders of a state should, as a general rule, inhibit a court's ability to impose restrictions upon the accessibility of online content in another state. However, Paul Schiff Berman provides a convincing counter argument against those in favour of limiting jurisdiction to the state, stating:

> ... one does not need to believe in the death of the nation-state to recognize both that physical location can no longer be the sole criterion for conceptualizing legal authority and that nation-states must work within a

[152] Brendan Van Alsenoy and Marieke Koekkoek "Internet and Jurisdiction after Google Spain: The Extra-Territorial Reach of the EU's "Right To Be Forgotten" (Working Paper No. 152, March 2015) at 15.
[153] A29WP *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain And Inc V. Agencia Española De Protección De Datos* (AEPD) and Mario Costeja González" C-131/12 (WP 225, 26 November 2014) at 3.
[154] Pippa Rogerson "Kuwait Airways Corp V Iraqi Airways Corp: The Territoriality Principle in Private International Law--Vice or Virtue?" (2002) 55 CLP 265 at 265.
[155] Brendan Van Alsenoy and Marieke Koekkoek "The territorial reach of the "right to be forgotten": think locally but act globally?" European Law Blog <europeanlawblog.eu>.
[156] Susan Kuchinskas " Google Axes Hate News" (23 March 2005) Internet News <www.internetnews.com>.
[157] Brendan Van Alsenoy and Marieke Koekkoek "The territorial reach of the "right to be forgotten": think locally but act globally?" European Law Blog <europeanlawblog.eu>.

> framework of multiple overlapping jurisdictional assertions by state, international, and even nonstate communities.[158]

Furthermore, when one considers the debate in the context of the facts of a particular case like *Costeja*, justifications can be found for global modification of search results. In this case, if the AEPD determined to go after the source of the publication there is a potential that La Vanguardia would have been ordered to remove the auction notices complained of, the practical effect of which would have been that the information would be rendered globally inaccessible.

2 Global jurisdiction

The French case *UEJF And LICRA V. Yahoo! and Yahoo France*[159] highlights the difficulties of global internet jurisprudence and has been said to "mark the beginning of the end of the no-sovereignty illusion" in the context of the Internet.[160] In this case, *Yahoo!* was sued for hosting an auction page displaying Nazi paraphernalia. The auction page was available to be searched from anywhere in the world including France, where the display of Nazi paraphernalia is outlawed. The Tribunal de Grande Instance (TGI) in France determined that *Yahoo!* should take all appropriate measures to prevent French nationals from accessing the page in question.[161] *Yahoo!* contended that it was impossible to comply with such an order and decided to take up its case in the United States. Judge Fogel in the United States District Court for the Northern District of California concluded that there are no international standards on the governance of online content and the TGI's decision was inconsistent with the American First Amendment right relating to freedom of expression.[162] However, this decision was later overturned by an en banc panel of the US Court of Appeals for the Ninth Circuit[163] on the basis that *Yahoo!*'s claim was not "ripe for adjudication".[164]

---

[158] Paul Schiff Berman *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders (Introduction)* (Cambridge University Press, Washington, 2012) at 4.
[159] *La Ligue Contre Le Racisme et l'antisémitisme* (LICRA) *v. Yahoo! Inc. and Yahoo! France* (Tribunal de Grande Instance de Paris, 2000).
[160] Raphael Cohen-Almagor "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications" (Thesis, Rochester Institute of Technology, 2011) at 1.
[161] *La Ligue Contre Le Racisme et l'antisémitisme (LICRA) v. Yahoo! Inc. and Yahoo! France*, above n 159.
[162] *Yahoo! Inc. v. La Ligue Contre le Racisme Yahoo! Inc* 169 F. Supp. 2d 1181; 2001 US Dist. Lexis 18378.
[163] Raphael Cohen-Almagor "Freedom of Expression, Internet Responsibility, and Business Ethics: The Yahoo! Saga and Its Implications" (Thesis, Rochester Institute of Technology, 2011) at 5.
[164] *Yahoo! Inc. v. LICRA and UEJF,* 433 F 3d 1199 (9th Cir. 2006).

In *Equustek Solutions Inc. v. Jack* (*Equustek*), the Supreme Court of British Columbia issued a global injunction against Google.[165] In this case, Google was not a party to the proceedings but became embroiled in the litigation through a third party interim injunction issued against them. Equustek argued that it was engaged in a game of "whac-a-mole" with Jack, a virtual company that had been found guilty of theft of trade secrets from Equustek. [166] Instead of complying with court orders to remove its online advertisements, Jack was carrying on its business through "a complex and ever expanding network of websites".[167] Equustek sought a third party interim injunction against Google on the basis that it considered Google to be facilitating Jack's on-going breach of court orders by continuing to provide hyperlinks to Jack's websites.

The Honourable Madam Justice Fenlon referred to *Costeja* in reaching her conclusion that: "Google is an innocent bystander but it is unwittingly facilitating the defendants' on-going breaches of this Court's orders."[168] In this case, the Court determined that it had the authority to issue an injunction with a global reach. It reasoned that removal of results from google.ca alone was inadequate to offer the plaintiffs effective relief.[169] There have been a number of criticisms of this decision. Statements have been made asserting that the decision highlights the necessity of a "principled debate as to the extent to which local decisions should be allowed to hamstring the global internet."[170] However, it cannot be argued that in the arena of online governance, an international shift away from tying jurisdiction to the state territory is emerging.

On the question of whether Google will be required to broaden its practice of de-indexing following the *Costeja* ruling, the answer will depend on the effectiveness of current practice in achieving compliance with the ruling.[171] In any case, the international attention that *Costeja* has received and its reference in cases like *Equustek*, will nevertheless mean that it will be influential in discussions on global internet jurisdiction that will emerge in the coming years.

---

[165] *Equustek Solutions Inc v Jack* (2013) BCSC 1063.
[166] *Equustek Solutions Inc v Jack,* above n 165, at [72].
[167] At [7].
[168] At [156] per Madam Justice Fenlon.
[169] At [75].
[170] Ren Bucholz of Lenczner Slaght Royce Smith Griffin LLP in Toronto: "B.C. ruling on jurisdiction over Google 'disastrous'" (22 June 2015) Law Times <www.lawtimesnews.com>.
[171] Brendan Van Alsenoy and Marieke Koekkoek "Internet and Jurisdiction after Google Spain: The Extra-Territorial Reach of the EU's "Right To Be Forgotten" (Working Paper No. 152, March 2015) at 30.

IV: DEVELOPMENTS AND RECOMMENDATIONS

As articulated by Lawrence Lessig "[b]ehaviour in the real world – this world, the world in which I am now speaking – is regulated by four sorts of contraints. Law is just one of those four constraints."[172]

A. Lessig's four regulatory constraints

The law is unable to undertake the sole responsibility of fast paced technological change. Many commentators have affirmed the Lessig approach to internet regulation. Lessig describes the way online regulation is improved where the following constraints are operating together: [173]

1. The law.
2. Architecture.
3. Social norms.
4. The market.

This combined approach will be explored. This exploration will incorporate an assessment of the GDPR, part of the EU's new legal solution to regulating online technologies. It will first focus on the GDPR's forecasted effect on SEOs and data subjects.[174]

1 The law: the new General Data Protection Regulation

The GDPR is one piece of the reform puzzle in the European Commission's 'Digital Agenda' for Europe.[175] The creation of a vibrant 'Digital Single Market' is the cornerstone of the digital agenda. The Digital Single Market is built upon the following pillars:[176]

1. Improving both consumer and business access to digital goods and services.
2. Creating a level playing field for digital networks and new technologies to enable their growth.
3. Capitalising on the digital economy.

[172] Lawrence Lessig "The Laws of Cyberspace" (essay presented at the Taiwan Net 1998 conference, Taipei, March 1998) at 2.
[173] At 4.
[174] See Chris Conley "The Right to Delete" (Presented at the AAAI Spring Symposium Series: Intelligent Information Privacy Management, California, March 2010) at 58.
[175] "Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market" Europa Nu <www.europa-nu.nl>.
[176] European Commission *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe* (COM 192 final, 6 May 2015) at 3.

The economic incentives of the Digital Single Market incorporate an understanding that there must be a strong level of privacy protection for personal data. The data protection framework has the objective of guaranteeing an approach to data privacy for EU citizens that also promotes certainty for business. This signals a continuation of the dual aims behind the data protection framework in the EU, as were mentioned in Chapter I.

The GDPR was spurred on by the the increased risk to privacy that technological advancements like the "growth of social networking and big data analytics" threaten to have.[177] The European Commission declared that the *Costeja* ruling "confirmed the main pillars of the data protection reform."[178] The A29WP described the GDPR's purpose as being to "reinforce the position of data subjects, (and) to enhance the responsibility of controllers."[179] The GDPR was first drafted by the Commission on 25 January 2012. The EU's legislative and executive bodies are currently negotiating its final format.[180] This regulation is set to be finalised early 2016 but will not come in to force until 2017 or 2018. The following comparison between the DPD and the proposed GDPR is primarily based on the European Commission text but it makes note of significant amendments made by the European Parliament in its legislative resolution of 12 March 2014.[181]

Two key features of the GDPR that will not differ from those of the DPD are:

1. Application of the law to personal data.[182]
2. Responsibility for compliance is allocated to the data 'controller.' However, the 'processor' will have obligations as well. These defined terms are identical to those found in art 4 of the DPD.

[177] Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers", above n 36.
[178] "Factsheet on the "Right to be Forgotten" ruling" European Commission <ec.europa.eu>.
[179] A29WP *Opinion 01/2012 on the data protection reform proposals* (WP 191, 23 March 2012) at 4.
[180] There are three texts at present: the commission text, the parliament text and the council texts, the commission text was the genesis of the regulation and has formed the starting point for the other texts: Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers", above n 36; The European Parliament is the law-making body of the EU. It passes laws together with the Council of the EU based on the European Commission's proposals: "European Parliament" European Union < europa.eu>.
[181] European Parliament *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)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), 12 March 2014).
[182] At 98, art 4.

The *Costeja* ruling that confirmed that Google is a data controller will apply as precedent under the GDPR and therefore SEOs will be subject to comply with and liable under the GDPR. However, the inclusion of liabilities under the GDPR for processors of information will affect the balance of responsibilities between data controllers and processors.

Whilst the above features remained unaffected, there are some key features of the GDPR that will affect how SEOs conduct their business that differ greatly from the way SEOs are expected to handle their data processing under the DPD. These relate to:

(i) Territorial Scope

Article 3 The GDPR proposes that it will apply to controllers outside of the EU so long as they offer "goods or services" to EU citizens irrespective of whether a payment... is required.[183] This may lead to liability for businesses that market products to EU citizens online.

(ii) Fines

The GDPR introduces heavy new penalties including fines of up to the greater of one million euro or two to five per cent of the controller's the annual worldwide turnover. This has been described as "as significant as antitrust in terms of compliance risk."[184] These fines are significantly greater than the maximum penalties that have generally been comparatively low under the DPD.[185] There is potential that these fines have a chilling effect on how SEO businesses operate in the EU. These sorts of fines could be particularly crippling for both small businesses and SEOs that engage in processing activities. This could work against the European Commission's objective of creating a level playing field for businesses in order to foster economic growth.

(iii) "One-stop-shop"

[183] European Commission text *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)* (COM(2012)0011), art 3.
[184] Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers", above n 36.
[185] Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers" above, n 36.

In an attempt to enhance certainty for businesses, every state will be required to have a Supervisory Authority.[186] These Authorities will have specific enforcement powers[187] which will be determined by the state[188]. Where a business has multiple establishments, it will be assigned a 'lead authority' based on the location of its main establishment.[189] This should work to improve certainty for businesses in relation to the data protection requirements that need to be followed in the various states. However, it is unclear how the lead authority will be assigned or what, if any, support will be offered by them to the controller that they are assigned.

The new GDPR makes some key changes to the rights of data subjects in the EU. These include:

(i) Right to erasure

Article 17 expands on the right to removal already available under the DPD. It grants individuals the "right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data." This expansion is primarily effected through reference to the art 19 right to object and the art 6 list of lawful bases for processing. The European Commission's proposal initially had titled art 17 the 'right to be forgotten and to erasure' but the European Parliament vote peeled this back to the 'right to erasure,' likely because the former is misleading.[190] The European Commission made it clear that the right to erasure is "not tantamount to deleting content" but rather entails data controllers like SEOs removing irrelevant and outdated links.[191]

However, as was was demonstrated by *Mosley v Google Inc & Anor*[192], there are many practical difficulties associated with vindicating ones privacy interests in the amorphous context of the Internet. Erasure of links "in an open system where anyone can produce a copy of the information once legally published"[193] cannot guarantee foolproof disassociation between the data subject and the online information complained of. The European Commission has yet to elaborate on how SEOs will be expected to implement full

[186] European Commission, above n 183, art 46.
[187] Art 53.
[188] Art 28.
[189] Art 51.
[190] "European, above n 183, art 4.
[191] "Factsheet on the "Right to be Forgotten" ruling" European Commission <ec.europa.eu>.
[192] *Mosley v Google Inc & Anor* [2015] EWHC 59.
[193] Pancani "Searching to be Forgotten: An Investigation of the Effects of the Proposed "Right to be Forgotten and to Erasure" on Search Engines" (Law & Technology Master Thesis, Tilburg Law School, 2013) at 61.

erasure.[194] However, in *Mosley*, Mitting J noted that "existing technology permits Google, without disproportionate effort or expense, to block access to individual images, as it can do with child sexual abuse imagery"[195] and by this, it can be inferred that Google (and potentially other SEOs) has the algorithmic means to identify and either block or erase particular information, preventing that information from being linked in search results complained of.

(ii) Right to object

Article 19 is functionally the same as the DPD's art 14(a) which refers to allowable bases for processing listed in art 7(f). Article 6(1)(f), to which art 19 refers, includes a new allowable objection to processing, namely where it is necessary for the "vital interest" of the data subject. No further specification about what constitutes vital interest has been made in the GDPR but it expands the basis for allowable objections. The European Parliament text has expanded this to cover vital state interests such as national security, law enforcement and public security[196], though the GDPR will require more transparency in relation to what these cover.

Article 17(3) articulates exemptions from erasure. While the data controller is required to promptly carry out the erasure, there are several possible exemptions including freedom of expression, health, research and compliance with union or member state law. This is a structural change from the DPD. The DPD provides for rectification where processing is non-compliant with the directive, which means there is no need for exemptions. In *Costeja*, the Advocate General held that freedom of expression could be found amongst the allowable bases for data processing in art 7(f).[197] The GDPR has removed these interests from the scope of allowable processing, instead looking to a relationship test where the burden of proof falls to the controller to show a legitimate interest in processing.

Overall, the final formation of the GDPR remains unclear. However, it is clear that SEOs are still going to be the first points of contact for removal and potentially fined heavily if they wrongly determine removals. On this issue, Jonathan Zittrain asserts "the incentives are clearly lopsided [towards

[194] "Factsheet on the "Right to be Forgotten" ruling" above n 191.
[195] *Mosley v Google Inc & Anor*, above n 192, at 54.
[196] European, above n 183, amendment 12, recital 20.
[197] *Costeja*, AG Jääskinen, above n 55, at 95.

removal]" as there are no penalties under the GDPR for improper removals but significant fines for rejecting removal requests.[198]

A solution, which may work to combat the danger of illegitimate censorship, would be re-structuring the requests process so that a democratically accountable government authority makes the determinations on removal requests and refers its decisions to all SEOs so that the data subject's right to removal is asserted in relation to widest point possible to limit distribution of their information. This could provide a safe harbour from liability of sorts for the SEO, with fines only being imposed where the SEO did not comply with the removal order. This option does not appear to have been considered in any great detail by the executive and legislative bodies.

Alternatively, if greater transparency can be achieved in the removals process then concerns about SEOs illegitimately censoring might be eased. The open letter from academics suggests an unveiling of information by SEOs that can reasonably be divorced from individual circumstances and requests. These suggestions are attached in Appendix A.

2 Architecture: privacy by design and coding

(i) Privacy by design

Using Lessig's language, privacy by design is an architectural constraint in the regulation of personal data processing online. Privacy by design is preventative. It is "embedded into the architecture of IT and business systems"[199] so that privacy is the default setting for the way that data is handled.

Articles 23 and 33 introduce the requirement of 'Privacy by Design' into the GDPR. This cohesion between legal and architectural constraints will provide more effective regulation of personal data processing if implemented correctly. It is not a concept that appears in the DPD but it may play a key part in achieving greater privacy for individuals online. It will be the responsibility of businesses to "implement appropriate technical and organisational measures to protect the rights of data subjects and ensure complainace with the regulation."[200] The Council has marketed this new

[198] Jonathan Zittrain in Annie Pruitt "When forgetting isn't best: Zittrain discusses the 'Right to be Forgotten'" (31 August 2015) Harvard Law <today.law.harvard.edu>.
[199] Ann Cavoukian "Privacy by Design: The 7 Foundational Principles" (August 2009) <www.ipc.on.ca>.
[200] Hunton & Williams "The Proposed EU General Data Protection Regulation: A guide for in-house lawyers", above n 36.

approach as a way for businesses to brand their service as one that is privacy conscious.

Data protection impact assessments will be involved in the change to privacy by design and will provide businesses with a mechanism designed to: (i) assess the privacy risks related to a proposed data processing activity; and (ii) identify measures to address these risks and demonstrate compliance with the regulation.[1] These impact assessments have been described by the European Parliament as "the essential core of any sustainable data protection framework" which can "fundamentally limit" privacy intrusive data breaches if they are thorough.[1] However, it must be noted that it could be difficult to conduct such an assessment in relation to the information processed by SEOs as they cover virtually all of the information available on the Internet.

(ii) Coding

Coding in the form of attaching a expiry date to data is another mechanism through which privacy of personal information may be increased.[201] Such a mechanism would, from the user's perspective allow the "ex-ante exercise of the right to be forgotten."[202] In order to implement coding, a "deletion manager" has been envisaged by the technologically savvy. This mechanism would "automate the process of deleting records by identifying and interacting with record-holding parties [and] track the flow of records from one party to another." However, there are difficulties associated with this kind of coding.[203] Coding necessitates that users are able to forecast how long they would like the life expectancy of personal data to be, which may prove impracticable in many instances, particularly where the user's decision may conflict with the purposes of controllers being satisfied.[204] Further, publishers of information concerning third party data subjects may not be amenable to coding expiry dates on the information where there is no legal requirement to do so.[205] If the requirement of coding was incorporated as an extension of the privacy by design requirement in the GDPR it could become part of the privacy compliant way that data will be required to be handled by businesses. If we relate this

[201] Viktor Mayer-Schoenberger, "Beyond copyright managing information rights with DRM" (2006), in 84 Denver University Law Review 181, at 182-184.
[202] Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice' (2012) 8(3) Tilburg Law School Legal Studies Research Paper Series 1, at 14 as cited in Alessandro Pancani "Searching to be Forgotten: An Investigation of the Effects of the Proposed "Right to be Forgotten and to Erasure" on Search Engines" (Law & Technology Master Thesis, Tilburg Law School, 2013) at 27.
[203] Conley, above n 174, at 57.
[204] Panacai, above n 41, at 27.
[205] Conley, above n 174, at 57.

idea back to the Costeja case, an expiry date could have potentially been set by the government body that had ordered the recovery of social security debts, for the time at which Mr González's property was auctioned off.

3 Social norms

Though it is clear that data subjects are not always the authors of the information on the Internet that relates to them, there seems to have been a shift in the social norm toward freely offering up personal information online. Facebook co-founder Mark Zuckerberg has described privacy as being over, due to a shift in social norms and the advent of social networking: [206]

> People have really gotten comfortable not only sharing more information and different kinds, but more openly and with more people. [This is a] social norm that has evolved over time.

Danah Boyd speaking at an international data protection conference stressed that there is "… no technical or legal silver bullet to social privacy." She states that there is a need to realise that "[i]n online public spaces, interactions are public-by-default, private-through-effort."[207] What she is trying to communicate is that people need to become more aware that the information that they offer up on to the Internet is searchable and can be aggregated, allowing searchers to make assumptions about their lives. If a greater number of initiatives like the "Workshop on Online Privacy and Consent"[208] was offered to the general public, increased internet literacy and awareness of the benefits of self-regulation and exercising more discretion could result.

4 The market

The digital market is characterised by its high level of personalisation and generally free services. There are a "[l]ack of economic incentives" for businesses to improve their privacy commitments. This is attributable to "the paradoxical attitude of... users" who, despite their concerns, tend to agree to vague privacy policies. [209] Further, participating the digital market often requires one to reliquish control over personal data. We must ask ourselves, while there is no actual monetary exchange, does engaging with the digital

[206] Mark Zuckerberg in Bobbie Johnson "Privacy no longer a social norm, says Facebook founder" (11 January 2010) The Guardian <www.theguardian.com>.
[207] Danah Boyd "The Future of Privacy: How Privacy Norms Can Inform Regulation" (International Conference of Data Protection and Privacy Commissioners, Israel, October 2010).
[208] "2015 Workshop on Online Privacy and Consent - #MCDE15" University of Southampton < www.southampton.ac.uk>.
[209] Panacai, above n 41, at 24.

market come at a huge cost? Many of the solutions offered by changes in the market or to social norms will rely on the free choice of the users.

Conclusion

The GDPR is the EU's legal answer to the regulation of data processing. Though many of the proposed changes will be beneficial for privacy, they may be crippling for businesses and could potentially result in illegitimate censorship by SEOs. As has been discussed, some key issues associated with the GDPR in its current format need to be addressed and ultimately, there is a need to take a four-cornered approach to achieve effective regulation. Architectural and legal constraints have a "direct and immediately significant impact on the issue" of online content regulation and behavioural changes for users are also necessarily part of the answer for improving privacy online. As has been articulated by Chris Conley:[210]

> The answer to the request for more control is a combined approach involving social norms, market, technical instruments and legal provisions, which takes into account the other existing laws and technologies.

[210] Conley, above n 174, at 58.

Conclusion

The ubiquitous role of SEOs on the Internet demands that these online actors take on some privacy obligations for the way in which they handle the processing of personal data. Undoubtedly, SEOs have a measure of control over achieving the balance between freedom of expression and the right to privacy in the online world. However, the law is notoriously unable to regulate fast-paced technological change in an effective manner. This has meant that the operations of SEOs have been left largely undefined and uncontrolled at the EU data protection law level.

The CJEU's ruling in *Costeja* establishes a precedent for SEO liability under the DPD. The profit-driven algorithmic programming that SEOs engage in, satisfies the data 'controller' definition in the DPD, by the reasoning that SEO algorithmists are in total control over the means and purposes of data processing. While the CJEU's approach to handling SEOs in *Costeja*, is forward-looking and correctly identifies SEOs as playing an active role in the online information economy, the CJEU in this case failed to provide clear guidelines on how SEOs are expected to implement its decision. As a result, the processes that SEOs have used to conduct removals have been void of real transparency. It is concerning that an SEO, a private company with an economic interest in streamlining the removals process, has been made the first point of contact for data subjects who wish to have results that concern them de-indexed.

The GDPR does not address the aforementioned issues. In fact, the new heavy fines for non-compliance with its provisions that have been proposed in the various draft texts of the GDPR, will only work to exacerbate the potential for illegitimate censorship. Instead of providing better clarification on controller liabilities and better protection for individual privacy interests, the GDPR, in its current format, imports uncertainty. In order to better regulate data controllers in the digital economy and provide more certainty for data subjects, co-operation between governments and these various online actors is required. Furthermore, changes to social norms and the operations of the market will help to limit the amount of online information that is able to be aggregated about a data subject. A purely legal response is not the solution.

Bibliography

A. Cases

1. Australia

Trkulja v Google Inc LLC & Anor (No 5) [2012] VSC 533.

2. Canada

Equustek Solutions Inc v Jack (2013) BCSC 1063.

3. EU

Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] OJ 212.

Case C-101/01 *Lindqvist* [2003] ECR I-12971.

Case C-70/10 *Scarlet Extended* [2011] ECR I-11959.

4. France

La Ligue Contre Le Racisme et l'antisémitisme (LICRA) *v. Yahoo! Inc. and Yahoo! France* [2000] TGI.

5. United States of America

Yahoo! Inc. v. La Ligue Contre le Racisme Yahoo! Inc [2001] 169 F. Supp. 2d 1181; US Dist. Lexis 18378.

Yahoo! Inc. v. LICRA and UEJF, [2006] 9th Cir. 433 F 3d 1199.

6. United Kingdom

Mosley v Google Inc & Anor [2015] EWHC.

B. Legislation

1. EU

Directive 95/46/EC (DPD) of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (DPD) [1995] OJ L 281.

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L 201.

Directive 2006/24/EC of the European Parliament and of the Council [2006] OJ L 105.

C. Proposed Legislation

European Commission *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe* (COM 192 final, 6 May 2015).

European Parliament *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)* (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD), 12 March 2014).

D. Books and Chapters in Books

Allen Baddeley *Human Memory: Theory and Practice* (Revised ed, Psychology Press Ltd, Bristol, 1997).

Aidan O'Neill QC *EU Law for UK Lawyers* (Hart Publishing Ltd, Oxford (UK), 2011).

Jorge Luis Borges *Funes el Memorioso* (Emece Editores, Argentia, 1956) (translated ed: Anthony Kerrigan (translator) Jorge Luis Borges *Ficciones* (Grove Press, New York, 1962).

Klaus-Dieter Borchardt *The ABC of European Union law* (Publications Office of the European Union, Luxembourg, 2010).

Laura Denardis "The Emerging Field of Internet Governance" in William H. Dutton *The Oxford Handbook of Internet Studies* (Oxford University Press, 2013).

Murray Laver *Computers and Social Change* (Cambridge University Press, New York, 1980).

George Orwell *1984* (Harcourt Brace Jovanovich, New York, 1949).

Paul Schiff Berman *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders (Introduction)* (Cambridge University Press, Washington, 2012).

Viktor Mayer-Schönberger *Delete: The Virtue of Forgetting in the Digital Age* (Princeton University Press, New Jersey, 2009).

Daniel J Solove *The digital person: technology and privacy in the information age* (New York University Press, New York, 2004).

Emanuele Tarantino "A note on vertical search engines' foreclosure" Joseph E. Harrington Jr and Yannis Katsoulacos (eds) *Recent Advances in the Analysis of Competition Policy and Regulation* (Edward Elgar Publishing, Cheltenham (UK), 2012).

E. Opinions, Papers and Reports

A29WP *Opinion 2/2010 on online behavioural advertising* (WP 171, 22 June 2010).

A29WP, *Opinion 1/2008 on data protection issues relating to search engines* (WP 140, 4 April 2008).

A29WP, *Opinion 1/2010 on the concepts of 'controller' and 'processor'* (WP 169, 16 February 2010).

A29WP *Opinion 01/2012 on the data protection reform proposals* (WP 191, 23 March 2012).

A29WP *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain And Inc V. Agencia Española De Protección De Datos (AEPD) and Mario Costeja González* C-131/12 (WP 225, 26 November 2014).

Case C-131/12 *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] OJ 212, Opinion of AG Jääskinen.

Bert-Jaap Koops, 'Forgetting Footprints, Shunning Shadows. A Critical Analysis of the "Right To Be Forgotten" in Big Data Practice' (2012) 8(3) Tilburg Law School Legal Studies Research Paper Series 1.

Committee on Legal Affairs and Human Rights *European Union and Council of Europe human rights agendas: synergies not duplication!* (Parliamentary Assembly, Doc. 13321, 2 October 2013).

Viktor Mayer-Schönberger "Useful Void: The Art of Forgetting in the Age of Ubiquitous Computing" (Faculty Research Working Papers Series No. 22, John F.Kennedy School of Government - Harvard University, 2014).

SS McCarty-Snead and AT Hilby *Research Guide to European Data Protection Law* (Legal Research Series Paper 1, Berkeley Law Scholarship Repository, 2013).

Brendan Van Alsenoy and Marieke Koekkoek "Internet and Jurisdiction after Google Spain: The Extra-Territorial Reach of the EU's "Right To Be Forgotten" (Working Paper No. 152, March 2015).

F. Journal Articles

David Lindsay "The 'Right to be Forgotten' by Search Engines under Data Privacy Law: A Legal Analysis of the Costeja Ruling" (2014) 6 JML 159.

Orla Lynskey "From Market-Making Tool to Fundamental Right: The Role of the Court of Justice in Data Protection's Identity Crisis" in Serge Gutwirth, Ronald Leenes, Paul de Hert and Yves Poullet (eds) *European Data Protection: Coming of Age* (Springer Dordrecht Heidelberg, New York, 2013).

Jonathan Zittrain "A History of Online Gatekeeping, Harvard Journal of Law and Technology" (2006) 19 Harvard JOLT 253.

Pippa Rogerson "Kuwait Airways Corp V Iraqi Airways Corp: The Territoriality Principle in Private International Law--Vice or Virtue?" (2002) 55 CLP.

Viktor Mayer-Schoenberger, "Beyond copyright managing information rights with DRM" (2006), in 84 Denver University Law Review 181.

G. Conferences

Danah Boyd "The Future of Privacy: How Privacy Norms Can Inform Regulation" (International Conference of Data Protection and Privacy Commissioners, Israel, October 2010).

Chris Conley "The Right to Delete" (Presented at the AAAI Spring Symposium Series: Intelligent Information Privacy Management, California, March 2010).

Lawrence Lessig "The Laws of Cyberspace" (essay presented at the Taiwan Net 1998 conference, Taipei, March 1998).

H. Newspaper Articles

Kate Connolly "Right to erasure protects people's freedom to forget the past, says expert" *The Guardian* (online ed, Berlin, 4 April 2014).

Lev Grossman "You Have the Right to Be Forgotten" *TIME* (online ed, New York, 26 May 2014).

Amir Mizroch "What Is the 'Right to Be Forgotten?'" *Wall Street Journal* (online ed, London, 13 May 2014).

Jeffrey Toobin “The Solace of Oblivion” *The New Yorker* (online ed, New York, 29 September 2014).

I. Internet Resources

“Ads in Gmail” Google <support.google.com>.

“Article 29 Working Party” European Data Protection Supervisor <secure.edps.europa.eu>.

Aidan O’Neill QC “How the CJEU uses the Charter of Fundamental Rights” (3 April 2012) Eutopia Law < eutopialaw.com>.

Ann Cavoukian “Privacy by Design: The 7 Foundational Principles” (August 2009) <www.ipc.on.ca>.

Byung-Cheol Kim and Jin Yeub Kim “The Economics of the Right to be Forgotten” (16 March 2015) <econ.msu.edu>.

Brendan Van Alsenoy and Marieke Koekkoek “The territorial reach of the “right to be forgotten”: think locally but act globally?” European Law Blog <europeanlawblog.eu>.

“Combat Negative Search Results With Reputation-Defender ®” Reputation.com <www.reputation.com>.

“Data Protection Day 2015: Concluding the EU Data Protection Reform essential for the Digital Single Market” Europa Nu <www.europa-nu.nl>.

“EU member countries” European Union <europa.eu>.

“European Union legal acts” (29 June 2010) EUR-Lex <eur-lex.europa.eu>.

“European privacy requests for search removals” Google Transparency Report < www.google.com>.

“European Parliament” European Union <europa.eu>.

Ellen P. Goodman “Dear Google: open letter from 80 Internet Scholars: Release RTBF Compliance Data” Medium < medium.com>.

“Factsheet on the “Right to be Forgotten” ruling” European Commission <ec.europa.eu>.

“FAQ: How are you implementing the recent Court of Justice of the European Union (CJEU) decision on the right to be forgotten?” Google Privacy & Terms < www.google.se>.

“Googlebot” Search Console Help <support.google.com>.

Hunton & Williams “The Proposed EU General Data Protection Regulation: A guide for in-house lawyers” (June 2015) <www.huntonregulationtracker.com>.

Jef Ausloos “The Right to be Forgotten – It’s about time, or is it?” (24 January 2004) Tech, Policy and Society <jefausloos.wordpress.com>.

Jonathan Owen “Is Google sabotaging the ‘right to be forgotten’?” (4 July 2014) New Zealand Herald <www.nzherald.co.nz>.

Jonathan Zittrain in Annie Pruitt “When forgetting isn’t best: Zittrain discusses the ‘Right to be Forgotten’” (31 August 2015) Harvard Law <today.law.harvard.edu>.

Kimberley Vogel “Google’s Targeted Keyword Ad Program Shows Strong Momentum with Advertisers” News from Google <googlepress.blogspot.co.nz>.

Loek Essers “This is how Google handles ‘right to be forgotten’ requests” (19 November 2014) Computer World <www.computerworld.com>.

Mark Zuckerberg in Bobbie Johnson “Privacy no longer a social norm, says Facebook founder” (11 January 2010) The Guardian <www.theguardian.com>.

“OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” *OECD* < oecd.org>.

Peter Sondergaard “Wake up to the Algorithm Economy” (5 August 2015) Gartner <www.gartner.com>.

“Regulations, Directives and other acts” European Union <europa.eu>.

“Request to Block Bing Search Results In Europe” <www.bing.com>.

Ren Bucholz of Lenczner Slaght Royce Smith Griffin LLP in Toronto: “B.C. ruling on jurisdiction over Google ‘disastrous’” (22 June 2015) Law Times <www.lawtimesnews.com>.

Rigo Wenning “The ECJ is right, the result is wrong” (16 May 2014) Internet Law: Online Legal Affairs 2.0 <www.internet-law.de>.

Robert Peston “Why has Google cast me into oblivion?” (2 July 2014) BBC News <www.bbc.com>.

“Search removal request under data protection law in Europe” Google Legal Help < support.google.com>.

“Streisand Effect” technopeadia <www.techopedia.com>.

Sandy Davidson “Right to be Forgotten” (11 June 2014) Jurist <jurist.org>.

Susan Kuchinskas “ Google Axes Hate News” (23 March 2005) Internet News <www.internetnews.com>.

“The Council of Europe’s Relations with the European Union” Council of Europe <www.coe.int>.

“The Value of Google Result Positioning (7 June 2013) Chitka Online Advertising Network <chitika.com>.

“The history of the European Union” European Union <europa.eu>.

“The reference for a preliminary ruling” (15 January 2014) EUR-Lex <eur-lex.europa.eu>.

“2015 Workshop on Online Privacy and Consent - #MCDE15” University of Southampton < www.southampton.ac.uk>.

J. Treaties

Statute of the Council of Europe EUTS 1 (opened for signature 5 May 1949, entered into force 3 August 1949).

Treaty of Maastricht on European Union OJ C 191 (opened for signature 7 February 1992, entered into force 1 November 1992).

K. Conventions

Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) CETS 005 (opened for signature 4 November 1950, entered into force 3 September 1953).

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS 108 (opened for signature 28 January 1981, entered into force 1 October 1985).

L. Charters

Charter of Fundamental Rights of the European Union (ECFR), 2000 OJ C 364/01.

M. Theses

Raphael Cohen-Almagor “Freedom of Expression, Internet Responsibility, and Business
Ethics: The Yahoo! Saga and Its Implications” (Thesis, Rochester Institute of Technology, 2011).

Alessandro Pancani “Searching to be Forgotten: An Investigation of the Effects of the Proposed "Right to be Forgotten and to Erasure" on Search Engines” (Law & Technology Master Thesis, Tilburg Law School, 2013).

Appendix A

1. Categories of RTBF requests/requesters that are excluded or presumptively excluded (e.g., alleged defamation, public figures) and how those categories are defined and assessed.
2. Categories of RTBF requests/requesters that are accepted or presumptively accepted (e.g., health information, address or telephone number, intimate information, information older than a certain time) and how those categories are defined and assessed.
3. Proportion of requests and successful delistings (in each case by % of requests and URLs) that concern categories including (taken from Google anecdotes): (a) victims of crime or tragedy; (b) health information; (c) address or telephone number; (d) intimate information or photos; (e) people incidentally mentioned in a news story; (f) information about subjects who are minors; (g) accusations for which the claimant was subsequently exonerated, acquitted, or not charged; and (h) political opinions no longer held.
4. Breakdown of overall requests (by % of requests and URLs, each according to nation of origin) according to the WP29 Guidelines categories. To the extent that Google uses different categories, such as past crimes or sex life, a breakdown by those categories. Where requests fall into multiple categories, that complexity too can be reflected in the data.
5. Reasons for denial of delisting (by % of requests and URLs, each according to nation of origin). Where a decision rests on multiple grounds, that complexity too can be reflected in the data.
6. Reasons for grant of delisting (by % of requests and URLs, each according to nation of origin). As above, multi-factored decisions can be reflected in the data.
7. Categories of public figures denied delisting (e.g., public official, entertainer), including whether a Wikipedia presence is being used as a general proxy for status as a public figure.
8. Source (e.g., professional media, social media, official public records) of material for delisted URLs by % and nation of origin (with top 5-10 sources of URLs in each category).
9. Proportion of overall requests and successful delistings (each by % of requests and URLs, and with respect to both, according to nation of origin) concerning information first made available by the requestor (and, if so, (a) whether the information was posted directly by the requestor or by a third party, and (b) whether it is still within the requestor's control, such as on his/her own Facebook page).
10. Proportion of requests (by % of requests and URLs) where the information is targeted to the requester's own geographic location (e.g., a Spanish newspaper reporting on a Spanish person about a Spanish auction).
11. Proportion of searches for delisted pages that actually involve the requester's name (perhaps in the form of % of delisted URLs that garnered certain threshold percentages of traffic from name searches).
12. Proportion of delistings (by % of requests and URLs, each according to nation of origin) for which the original publisher or the relevant data protection authority participated in the decision.
13. Specification of (a) types of webmasters that are not notified by default (e.g., malicious porn sites); (b) proportion of delistings (by % of requests and URLs) where the webmaster additionally removes information or applies robots.txt at source; and (c) proportion of delistings (by % of requests and URLs) where the webmaster lodges an objection.