COMMENT

GOOGLE SPAIN

Addressing Critiques and Misunderstandings One Year Later

Paul de Hert* and Vagelis Papakonstantinou**

§1. INTRODUCTION

Since the Court of Justice of the European Union (CJEU) handed its ruling in *Google Spain*[1] down last year, it has triggered an ongoing debate. This Journal made a kind invitation to continue a discussion that started in 3 *MJECL* (2014) with contributions by Christopher Wolf,[2] Hielke Hijmans[3] and Giovanni Sartor,[4] and in 1 *MJECL* (2015), by Christopher Kuner.[5] It is not only welcome but also timely.[6] In the year that passed since the judgment was rendered, the debate was kept alive not only at a theoretical level, with significant contributions by a number of authors on both sides of the Atlantic, but also at a practical level. Google's own interpretation and application of the Court's judgment was assessed by, and responded to, by individuals as well as Member State Data Protection Authorities (DPAs).

* Professor at VUB, LSTS; Tilburg, TILT.

** VUB, LSTS.

1 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, EU:C:2014:317.

2 C. Wolf, 'Impact of the CJEU's right to be forgotten: Decision on search engines and other service providers in Europe', 21 *MJECL* (2014).

3 H. Hijmans, 'Right to have links removed: Evidence of effective data protection', 21 *MJECL* (2014).

4 G. Sartor, 'Search engines as controllers: Inconvenient implications of a questionable classification', 21 *MJECL* (2014).

5 C. Kuner, 'Google Spain in the EU and international context', 22 *MJECL* (2015).

6 By way of summary of the other contributors' views, Wolf expresses concern about the decision's impact on the internet and on the freedom of expression online; Hijmans focuses on the decision's potential to effectively protect human rights in the EU; Sartor questions the Court's classification of search engines in particular with regard to the e-Commerce Directive (Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, [2000] OJ L 178/1); and Kuner places the Court's decision in the international context, examining it within the globalization of constitutional clashes framework.

In the text that follows the authors will first highlight some subjectively important facts that need to be kept under consideration while assessing the Court's decision against the business model currently employed by US internet companies (section 1). In section 2 the authors will engage with Sartor's concerns with regard to search engines being classified as 'data controllers'. Section 3 will deal with the issue of extraterritoriality, attempting to assess both Wolf's reservations and Hijmans' enthusiasm. The Court's balancing between economic interests and the right to data protection will be elaborated upon in section 4, while also attempting to address Peers' and Solove's criticism on the Court's balancing method. Finally, in section 5, the authors, in response to Kuner's idea of the globalization of constitutional clashes, will present their own thoughts on Google's actual implementation of the Court's decision for the past year and the DPAs' reaction to it.

In essence, the authors think that it constitutes more an exercise of the principle of proportionality than application of substantive data protection law: the Court applied the proportionality criterion in a successful manner given the circumstances at hand. However, these circumstances may easily be reversed in an internet world of versatility. Additionally, in the author's opinion, apart from well-identified issues such as geographical restrictions or administrator notification, a largely overlooked interest refers to the public's right to know and, if appropriate, to object. Essentially, search engines' delisting decisions ought to be challengeable not only by the individuals concerned in the event of a refusal, but also by the general public, in the event of an unjustified acceptance.

§2. SOME USEFUL FACTS: *EX ANTE* AND *EX POST* THE *GOOGLE SPAIN* DECISION

The actual case details (Mr Mario Costeja Gonzalez complained about embarrassing information online, both on the website of a Spanish newspaper and through Google search engine results) need not be repeated here. What is important is to keep in mind a number of facts that predated and followed the CJEU decision.

With regard to the former, one first needs to focus on the Google search engine: this is a marvel of engineering that automatically scans all of the internet and, for the time being, is able to churn out information on anyone and anything regardless of where this information may be hidden. Despite the technicalities, what is of interest (or, what is assessable by a court) is the ease of access: practically anyone can learn anything using the Google search engine, even if the information in question lies hidden in an obscure server in some remote corner of the world.

Competitors to Google's search engine do exist, but in Europe, Google accounts for more than 90% of internet searches.[7] This is because of the success of its search algorithm,

7 European Commission, Statement by Commissioner Vestager on antitrust decisions concerning Google, Brussels, 15 April 2015.

which by now has acquired mythical proportions. The user consensus is that the Google search engine will provide the most relevant results on a user question within the first few pages. Competitors are less successful in this regard. Consequently, Google is not a simple indexing service; it cares how (personal) information is processed. Its algorithm distinguishes and categorizes (personal) information: for instance, the search results for 'Mario Costeja Gonzalez' can relate mostly to the claimant and not to one of the millions others around the globe who share that name (per country server-separation, also performed by the Google algorithm, and also important to the same end). Of course, this is a basic function and the aim of every internet search engine that exists.

On the other hand, what was pioneered by Google but has found general application the meantime, refers to US internet companies' European data protection policies. The issue is of broader (non-Google-specific) relevance: over the past few years (Dropbox and Twitter being the latest addition to a long list), US internet companies have adopted a 'divide and conquer' EU data protection policy. Despite their sales availability and/or subsidiary presence in all EU countries, their data protection forum of preference, as set in the relevant terms of service, is not the respective Member State each time but invariably in Ireland or in the United Kingdom. This creates insurmountable difficulties for EU data protection implementation from the part of the individuals concerned: essentially, data subjects cannot file complaints against these companies with their own DPAs but have to travel to the above Member States instead. In a recent development, the Belgian Data Protection Commissioner drafted a lengthy 'recommendation' on the reasons why he sees himself as competent for data protection infringements committed by Facebook, despite the fact that the designated jurisdiction in the relevant terms of service is Ireland.[8] Until the problem is hopefully resolved in the future, the fact remains that US companies aim for the limits both of their internet sales models and the territorial scope of a directive drafted in 1995.[9]

§3. ON GOOGLE BEING A DATA CONTROLLER: WHAT IS A 'SEARCH ENGINE' ANYWAY? A REPLY TO SARTOR'S CONCERNS

Given the above, we are inclined to agree with the Court's finding that Google is indeed a 'data controller' within the meaning of the EU Data Protection Directive. A data controller is the one who 'determines the purposes and means of the processing

8 See Recommandation n° 04/2015 du 13 mai 2015 d'initiative concernant 1) Facebook, 2) les utilisateurs d'Internet et/ou de Facebook ainsi que 3) les utilisateurs et fournisseurs de services Facebook, en particulier les 'plugins' sociaux (CO-AR-2015–003).

9 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/1 (the EU Data Protection Directive).

of personal data' (Article 2(d) of the Directive). Although the Google search algorithm is automatic and in theory the Google search engine merely provides an indexing service, in practice Google categorizes and correlates (personal) data from all possible perspectives in order to present the most relevant search results within the first few pages it churns out after a search request. From this point of view it does not only index but also determines 'the purpose and means' of the processing of personal data. 'Knowledge' of the data controller or 'alteration' of the data, as Google contested, are not necessary conditions to this end.[10]

From this point of view, we believe that Sartor attaches too much attention to the option not to be indexed by search engines.[11] Indeed, non-indexation by search engines is a popular option on the internet that can be exercised either by the administrator (whole website not indexed) or by a single user (single profile not indexed). However this does not alter the fact that on what internet remains (the 'open' internet) indexation does take place by search engines. And after such indexation, Google applies its algorithms where indexed information is 'cleverly' correlated in order, for instance, to provide Mr Costeja Gonzalez's embarrassing information in the first few result webpages and not in the 1000th that no-one visits.[12] We believe that it is exactly this 'cleverness' of the Google algorithm (shared perhaps to a lesser extent by the algorithms of its competitors) on which its data controller status lies – or, if one prefers, its efficiency in the market was its demise in court.

In view of the above, we agree with the Court's conclusion that search engines are data controllers, but we nevertheless believe that the Court reached that conclusion through the wrong reasoning – a finding that might have future repercussions on the validity of the its decision. The Court did not properly assess the technical data explained above (section 3), but instead classified search engines as data controllers by application of the principle of proportionality: Search engines are data controllers because they play a 'decisive role' in the dissemination of information.[13] It is the quality of their service, not the technical details supporting it, that qualified search engines as data controllers.

However, in this way the *Google Spain* decision is practically undermined within a fast changing internet world. If, for instance, in the near future search engines cease to be 'decisive' in the dissemination of information (because Facebook is where personal data are located and, as everybody knows, Facebook and other social networks are not accessible to search engines), then the *Google Spain* decision automatically becomes

10 See C. Wolf, 21 *MJECL* (2014), p. 549. At any event, 'knowledge' of the data could be contested for Google – not of course by its employees, but by its algorithm that is designed to recognize information and correlate relevant bits of it.

11 See G. Sartor, 21 *MJECL* (2014), p. 568–570.

12 Customarily, any internet search returns millions of 'results', which, because they are organized in webpages of only a dozen, are practically and effectively unvisitable by internet users.

13 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 36.

obsolete. Or, even worse, is this decision at all applicable to internet search engines that are less successful than Google's, thus not holding such a 'decisive' role in the dissemination of information? In the same context, is *Google Spain* applicable to those search engines that offer increased privacy protection functions? All these questions need not have been raised if the Court had properly assessed the technical data on search engines and had based its classification on them rather than on the principle of proportionality.

§4. ON THE EXTRATERRITORIALITY EFFECT: ADDRESSING WOLF'S CONCERNS AND HIJMANS' ENTHUSIASM

A lot of criticism against the Court's decision has focused on the extraterritoriality effect given by the Court to EU data protection law. These arguments have also been echoed in Wolf's contribution: 'in effect, the ruling invites European regulators to force non-EU based businesses to conform their websites to comply with the EU data protection law just because they have a physical presence within the EU'.[14] On the other hand, Hijmans celebrated the Court's decision as 'evidence of effective data protection'. Perhaps the truth ultimately lies on whichever side of the Atlantic one resides. However, to our mind, the Court overcompensated as a fair reaction to a 'lawyeristic' stretching of EU law to its limits by US internet companies.

With regard to the applicable law, Article 4(1) of the Directive states that its provisions apply 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; (…)
(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

As it can be easily understood, this wording is particularly limiting in the internet age, but one should keep in mind that the Directive was drafted long before the internet entered our everyday lives. However, until it is replaced, the fact remains that applicable law requires 'an establishment' and processing executed 'in the context of' its activities in order for its provisions to develop their effect – even extraterritorial, if needed.

The Court therefore had to apply the above wording to Google's clever legal scheme of establishing marketing subsidiaries across the EU that only sell advertising and are

14 C. Wolf, 21 *MJECL* (2014), p. 547.

in no way themselves involved in the processing of personal data (see section 3). The Court quickly established that Google subsidiaries are 'an establishment' as per the Directive's requirements[15] – although to van Alsenoy and Koekkoek this is far from straightforward.[16]

Nevertheless, in order to establish personal data processing 'in the context of' these activities, and therefore to surpass Google's legal construction, the Court resorted entirely to teleological reasoning: 'in the light of the objective of Directive 95/46 of ensuring effective and complete protection of the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data, those words cannot be interpreted restrictively'[17] and

> it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented, by prescribing a particularly broad territorial scope.[18]

It only is in this way and not by strict interpretation of the law at hand that the *Google Spain* decision acquired its extraterritorial scope.[19]

Such an expansion of scope was hinted at by EU data protection's most staunch proponent, the Article 29 Working Party, in the past but had never been confirmed in practice. Back in 2010, an Opinion on applicable law was issued, according to which 'the decisive element to qualify an establishment under the Directive is the effective and real exercise of activities in the context of which personal data are processed',[20] while the 'degree of involvement' and the 'nature of the activities of the establishment' were suggested as the criteria in order to establish EU law applicability.[21] However, the Court did not apply these two criteria in its reasoning – had it done so, it would have perhaps reached an entirely different decision. Instead, the Court simply gave a broad interpretation of the Directive's wording, leaving aside any further specifying criteria.

In our view, the Court adopted a broad interpretation of the law in order to offer effective data protection to individuals. Its interpretation is perhaps compatible with the effects principle, as suggested by van Alsenoy and Koekkoek.[22] Ultimately, the Court's decision to

---

15 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 49.

16 See B. Van Alsenoy and M. Koekkoek, 'Internet and Jurisdiction after Google Spain: the Extraterritorial Reach of the "right to be delisted"', 5 *International Data Privacy Law* (2015), p. 109.

17 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 53.

18 Ibid.

19 Further elaboration of the Court's line of thinking can already be found in the Opinion of Advocate General Cruz Villalón in Case C-230/14 *Weltimmo*, EU:C:2015:426.

20 Article 29 Working Party Opinion 8/2010 on applicable law, [2010] WP 179.

21 Ibid., p. 10 et seq.

22 See B. Van Alsenoy and M. Koekkoek, 5 *International Data Privacy Law* (2015), p. 109.

consider Google's (and others', as seen in section 3) well-known business practice in Europe as lying within 'the context of the activities of an establishment of the controller' is perhaps difficult to justify on a *de lege lata* basis, but is explicable on the basis of the general EU personal data processing environment (*de lege ferenda*). It is perhaps in this context that Hijmans celebrates the decision as 'evidence of effective data protection'.[23] What Hijmans notes in particular with regard to the protection of fundamental rights on the internet is especially revealing: 'this case fits within a more general tendency in the Court's case law – especially following the entry into force of the Lisbon Treaty – to attach great importance to the effective protection of fundamental rights'.[24] However, is Hijmans right to be celebrating?

As regards the Court itself, Sweet has noted that 'the European Court, a Trustee of the Treaty system rather than a simple Agent of the Member States, operates in an unusually broad zone of discretion, a situation the Court has exploited in its efforts to enhance the effectiveness of EU law'[25] – a point that has been followed by a number of scholars until now.[26] Notwithstanding the application of this finding in other fields, in this particular case Kuner is certain that the Court 'will apply a strong fundamental rights analysis to data processing on the internet',[27] while Hijmans notes that 'the Court aims at ensuring that existing legal instruments remain effective for the protection of essential values, instead of getting rid of these instruments and giving up protection'.[28] The Court therefore intervened, in order to save individual data protection on the basis of an outdated instrument – the EU Data Protection Directive. While 'getting rid of' and 'giving up' is certainly not an option, particularly after the introduction of Article 16 TFEU, is the Court's 'aim' indeed commendable? In other words, is the correct way forward to stretch a 1995 wording to its limits in order to accommodate 2014 business practices? Would it not be preferable for the Court to note the law's limitations, drop the case for this reason, and ask for immediate legal action to remedy this? If we were to constantly 'adapt' the 1995 Directive to 2014 and beyond circumstances by stretching its wording are we not opening the gate to legal uncertainty and speculation? Ultimately, if we were to apply this practice interminably, is the EU data protection reform package at all useful? To our mind, data protection is a 'technical' human right in need of updated and case-specific auxiliary regulation. The Court's intervention to 'save the day' and the

23 H. Hijmans, 21 *MJECL* (2014).

24 Ibid., p. 556.

25 A. Stone Sweet, 'The European Court of Justice and the judicialization of EU governance', 5 *Living Rev. Euro. Gov.* (2010), p. 1.

26 See, for instance, D.R. Kelemen, *Eurolegalism: The Transformation of Law and Regulation in the European Union* (Harvard University Press, 2011); I. Spahiu, 'Courts: An Effective Venue to Promote Government Transparency? The Case of the Court of Justice of the European Union', 80 *Utrecht Journal of International and European Law* (2015). In this context, Kuner notes that a number of other important cases (the *EU-US Safe Harbor*, the *EU-Canada PNR agreement*) are also pending in front of the CJEU (C. Kuner, 22 *MJECL* (2015), p. 161).

27 C. Kuner, 22 *MJECL* (2015), p. 163.

28 H. Hijmans, 21 *MJECL* (2014), p. 557.

face of EU data protection hides regulatory shortcomings and applies soothing practices where immediate remedies are needed instead.

Finally, as correctly noted by van Alsenoy and Koekkoek,[29] jurisdictional issues surrounding the internet are by no means unprecedented: In fact, the *Google Spain* decision is only the latest addition to a long list of court disputes where local governments and courts fight bitterly over whose law applies over specific internet practices. The *Google Spain* decision is admittedly the first to bring data protection in this game – perhaps highlighting a 'clash of constitutional visions' as Kuner observes in his contribution.[30]

§5. THE CJEU'S BALANCING ACT: ADDRESSING CRITIQUES BY PEERS AND SOLOVE

While assessing the *Google Spain* decision, it is important to keep in perspective its real scope – as well as, what it actually asks Google to do. In the first place, the Court did not ask the Spanish journal, where the embarrassing information on the claimant appears, to remove the relevant webpages. Freedom of journalism aside, as Ausloos correctly notes,[31] the right to be forgotten can only be applied when the individual has consented to the processing and not whenever personal data has been lawfully obtained without the individual's consent. Equally important is the fact that the Court defined 'search engines' as providers 'of content which consists in finding information published or placed on the internet by third parties (…),'[32] meaning that self-serving search engine facilities (for instance, provided by online newspapers, magazines or even blogs) are not found within the scope of its decision.[33] Consequently, the freedom of journalism and the freedom of expression are not an issue here, despite the tremendous criticism this decision attracted on these grounds particularly on the other side of the Atlantic.[34] In addition, as noted both by Mantelero and Solove, a right to be forgotten with regard to media publications is not unknown both in Europe and in the USA.[35] Freedom of journalism and freedom

29 B. Van Alsenoy and M. Koekkoek, 5 *International Data Privacy Law* (2015), p. 114.

30 C. Kuner, 22 *MJECL* (2015), p. 160.

31 J. Ausloos, 'The "Right to be Forgotten" – Worth Remembering?', 28 *Computer Law & Security Review* (2012).

32 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 21.

33 See also Article 29 Data Protection Working Party, 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 (Article 29 WP Opinion), [2014] WP 225, para. 18.

34 See C. Wolf, 21 *MJECL* (2014), p. 552.

35 A. Mantelero, 'The EU Proposal for a General Data Protection Regulation and the Roots of the "Right to be Forgotten"', 29 *Computer Law & Security Review* (2013); and D. Solove, 'What Google Must Forget: The EU Ruling on the Right to Be Forgotten', *Linkedin* (2014), www.linkedin.com/pulse/20140513230300–2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten.

of expression are certainly protected in Europe as well, these two rights do not warrant fingertip information as well: if anybody wishes to form or express an opinion on Mr Costeja Gonzales, he might as well do the research to support it. Search engines do not express opinions and certainly do not exercise journalism (if that was the case, Google would not have struggled against its characterization as 'data controller' anyway). They are only auxiliary (indeed, not components) to the exercise of these, and several other, human rights. Consequently, their regulation has nothing to do with the above rights.

The *Google Spain* decision is an exercise of the principle of proportionality:[36] as per the Court's reasoning:

> processing of personal data, such as that at issue in the main proceedings, carried out by the operator of a search engine is liable to affect significantly the fundamental rights to privacy and to the protection of personal data when the search by means of that engine is carried out on the basis of an individual's name, since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet – information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty – and thereby to establish a more or less detailed profile of him. Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous.[37]

Subsequently, the Court weighted the above against Google's legitimate interest to process the information – also acknowledged in EU data protection law – but found an imbalance in the relationship: 'In the light of the potential seriousness of that interference, it is clear that it cannot be justified by merely the economic interest which the operator of such an engine has in that processing.'[38] Hence, Google's processing was found unlawful.[39] The use of such a proportionality reasoning in data protection matters is far from unusual for the Court. According to Tranberg, its application includes four tests: assessment of a measure's suitability, necessity, proportionality *stricto sensu* as well as whether a violation of a person's data protection right is justified.[40]

---

36 On the four stages of the proportionality test (the legitimate objective stage, the suitability stage, the necessity stage and the *stricto sensu* proportionality/balancing stage) see, for instance, E. Xanthopoulou, 'The Quest for Proportionality for the European Arrest Warrant: Fundamental Rights Protection in a Mutual Recognition Environment', 6 *New Journal of European Criminal Law* (2015).

37 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 80.

38 Ibid., para. 81.

39 See also the Article 29 WP Opinion, para. 5.

40 See C.B. Tranberg, 'Proportionality and data protection in the case law of the European Court of Justice', 1 *International Data Privacy Law* (2011).

Nevertheless, the Court did not go over all these steps in its *Google Spain* decision, probably because not all of them were needed. Instead, it simply balanced the potential consequences of this type of processing for individuals' rights against the search engines' financial interests and decided in favour of the former. In doing so, the Court simply applied the law at hand: the Directive allowed Google either the defence of its economic interests, as above, or that of 'journalistic purposes', as per Article 9 of the Directive, where indeed a balancing with the freedom of expression would have taken place. Nevertheless, because search engines are not 'publishers' of information,[41] the balancing against the freedom of expression never happened – to our mind a justified omission that, however, was heavily criticized by Peers[42] and others.

Solove suggested that when it comes to privacy, EU law focuses more on declaring fundamental principles; US law is more focused on balancing and practicalities: 'The US approach to privacy is pragmatic in that it reflects a balancing of privacy with other interests. It is much less concerned with articulating first principles.'[43] The foregoing shows in our opinion that the balancing has been done by the Court of Justice, albeit in a succinct manner.

In any event, the fact that the Court based its decision on the principle of proportionality and not on application of another data protection provision creates concrete consequences for the parties affected by it. The first one is quite obvious, but nonetheless noteworthy: internet search engines may continue to do what they do from an EU data protection perspective, subject of course to the right of individuals to have links pertaining to them removed. Things would have been different if, instead of the principle of proportionality, the Court had found Google's correlation of information as outright unlawful (for example, as not being a 'fair' collection and processing of data).

Second, the Court's decision is relative: if search engines as we know them cease to be so efficient on individual profiling in the future (because, for instance, they are shut out of online social networks' contents where most of the personal information residing on the internet is to be found), then the Court's decision might need reassessment. Terms used in the Court's reasoning such as 'modern society',[44] at least when used in the e-commerce context, hardly promote legal certainty. Equally, one notable shortcoming of the Court's decision is already visible: online social networks' internal search engines

41 See Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 35.

42 See S. Peers, 'The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression', *EU Law Analysis* (2014), http://eulawanalysis.blogspot.gr/2014/05/the-cjeus-google-spain-judgment-failing.html; S. Kulk and F.J. Zuiderveen-Borgesius, 'Google Spain v. González: Did the Court Forget About Freedom of Expression?', 3 *European Journal of Risk Regulation* (2014).

43 D. Solove, 'What Google Must Forget: The EU Ruling on the Right to Be Forgotten', *Linkedin* (2014), www.linkedin.com/pulse/20140513230300–2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten.

44 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 80.

are probably left out of its reach. Finally, the Court's decision is time-specific: because the internet has a history of only 20 years or less it is still possible to identify individuals relatively accurately on it. In other words, in another decade or two thousands of Spanish 'Mr Costeja Gonzalezes' will have been added to the internet, meaning identification of one in particular much more difficult. Again, under new circumstances the principle of proportionality will probably need re-evaluation.

In the same context, the *Google Spain* decision does not give individuals any 'right to be forgotten'.[45] As already explained, the Court of Justice did not ask for deletion of the original information. Notwithstanding the subtle distinction between a right to erasure and a right to oblivion,[46] the right to be forgotten at least as articulated under the EU data protection reform package[47] would essentially include a 'right to delete' or 'to have deleted'. According to the draft Article 17 of the General Data Protection Regulation, actual data is to be deleted – not third-party links to them. If we ultimately believe that by deleting Google links people forget, then we need to seriously reconsider the mechanics of human memory today and in the foreseeable future.

For the time being, individuals do have a right to 'delisting', meaning they can have links relating to them removed.[48] As will be seen in the analysis that immediately follows, they have since made use of this new option enthusiastically. It is therefore useful to examine the Court's criteria to this end. The centrepiece of the Court's ruling in this regard is laid down in paragraph 94:

> therefore, if it is found, following a request by the data subject (…) that the inclusion in the list of results displayed following a search made on the basis of his name of the links to web pages published lawfully by third parties and containing true information relating to him personally is, at this point in time, incompatible with (…) the directive because that information appears, having regard to all the circumstances of the case, to be 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, the information and links concerned in the list of results must be erased.

Consequently, a successful application for removal needs to establish that information is either 'inadequate', or 'irrelevant', or 'no longer relevant' or 'excessive'. If either one of these circumstances is identified, then a search engine needs to comply. The Court did not provide much additional guidance on this, apart from the 'public life' criterion:

---

45 See also The Advisory Council to Google on the Right to be Forgotten Report, 6 February 2015, (the Google Advisory Council Report), no. 2.

46 See, for instance, M.L. Ambrose and J.Ausloos, 'The Right to be Forgotten Across the Pond', 3 *Journal of Information Policy* (2013).

47 Comprised of the General Data Protection Regulation (COM(2012) 11 final), and a Directive on crime-related personal data processing (COM(2012) 10 final).

48 Term copied from the Google Advisory Council Report, no. 2.

> however, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.[49]

One could argue interminably with the Court's own application of this new right in paragraph 98. With regard to the claimant, although the Court found that 16 years are excessive for the embarrassing information to remain linked, a potential client or associate might argue differently. The same applies, for instance, to medical malpractice lawsuits.[50] Each of the authors, coming from different jurisdictions, can very easily identify examples of individuals who took immediate advantage of the Court's new right to have links removed where it would be for the benefit of society for the links to remain exactly where they are. 'Public life' does not quite help the distinction, because as everybody knows, modern life obscures the relationship between 'celebrities', 'public office', 'public life', 'anonymous users', and so on, with roles being freely exchangeable more than once over a single lifetime. Where is a line to be drawn? Should there even be one?

§6. POST SCRIPTUM: GOOGLE'S IMPLEMENTATION, THE DPAS' REACTION AND KUNER'S CONCERN ON THE GLOBALIZATION OF CONSTITUTIONAL CLASHES

Immediately after the decision was issued Google took action: it set up a relevant webpage to collect delisting applications and established an advisory board that travelled across Europe in meetings with interested parties. The Advisory Board issued its decision in early 2015.[51] On the other hand, the Article 29 Working Party issued an Opinion on the matter on November 2014,[52] providing guidelines to Member State DPAs on how to handle complaints by individuals (who evidently had their applications refused by Google). Individuals, on their part, embarked forcefully upon their newly acquired option to be delisted from the Google search engine (statistics, or even implementation in other search engines do not exist): within the first year more than 250,000 applications were made to Google. Recently, a number of European academics addressed an open

49 Case C-131/12 *Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, para. 97.

50 See A. Kassam, 'Spain's everyday internet warrior who cut free from Google's tentacles', *The Guardian* (2014), www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez.

51 The Google Advisory Council Opinion.

52 The Article 29 WP Opinion.

letter to Google, demanding more transparency on its handling of delisting requests.[53] The French DPA (CNIL) took it upon itself to force Google towards global delisting (see below).[54] Does this all amount to a globalization of a constitutional clash, which Kuner expresses to be a concern?

Expectedly, a number of issues have been raised over the first year of implementation of the *Google Spain* decision. Although the analysis of these issues largely exceeds the limits of this contribution, they deserve to be mentioned in brief here. The first refers to the balancing of fundamental human rights: Google is asked in a way to execute a court's (or, in the best case, a DPA's or in – any event – a state's) work. The Article 29 Working Party grossly underestimates Google's work, when it claims that 'despite the novel elements of the CJEU judgment, deciding whether a particular search result should be de-listed involves – in essence – a routine assessment of whether the processing of personal data done by the search engine complies with the data protection principle'.[55] Google's work, once it receives a delisting request, is not simply to establish whether data are sensitive or not or whether proper registrations have been made. In essence, Google needs to balance for each and every application whether data are 'inadequate, irrelevant or no longer relevant, or excessive' as well as whether any given individual in the EU has played a role in (local) 'public life'. More than anything, this task involves an assessment of case specificities and a balancing of fundamental human rights normally undertaken by courts or public authorities rather than private companies.

Executing this task for a quarter of a million individual applications per year is practically impossible (and a 'disproportionate effort' is an explicit concern in basic data protection law).[56] If it were to perform it in a satisfactory way, Google would have had to become acquainted with all the subtleties of each and every European local society. In order to properly execute this task, Google would have to perform 'interest balancing', as suggested by Alsenoy and Koekkoek,[57] but anything like that for 250,000 individual cases would be impractical at the least. Each country has thousands of individuals stepping in and out of public life at various stages of their lives: Google has to know about each one of them in order to properly assess the local public's interest to access information easily or not. This is practically an impossible task. If copyright bring-down notifications are any indication to this end, Google would probably prefer for this to be as automated as possible. On the other hand, the Article 29 Working Party even imagines search

53 See E.P. Goodman et al., 'Open Letter to Google From 80 Internet Scholars: Release RTBF Compliance Data', *Medium* (2015), https://medium.com/@ellgood/open-letter-to-google-from-80-internet-scholars-release-rtbf-compliance-data-cbfc6d59f1bd.

54 CNIL, 'CNIL orders Google to apply delisting on all domain names of the search engine', *Website of CNIL* (2015), www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/.

55 The Article 29 WP Opinion, para. 24.

56 See Articles 11 or 12 of the EU Data Protection Directive.

57 B. Van Alsenoy and M. Koekkoek, 5 *International Data Privacy Law* (2015), p. 117.

engines contacting original webmasters on the merits of specific case,[58] something that is logically impossible. Clearly, a balance needs to be struck for this unique role suddenly awarded to a single private company.

Of course, the issue that has attracted most attention is transparency. In fact, all three reports at hand still ask Google for more transparency on its handling of delisting applications. Evidently, transparency works two-ways: potential applicants need to know the Google delisting criteria. Also, the general public needs to know both of these criteria and the fact that delisting has been performed for a specific individual. Particularly the latter merits some further analysis: we believe that the public (internet users) needs to know that a specific individual has had links about him or her removed, although not the actual content of these links. A general disclaimer, as envisaged by the Article 29 Working Party,[59] probably in the same vein as the cookies notification of the e-Privacy Directive, is not sufficient. A right to know is crucial for challenging Google delisting decisions by the public, an equally important part of any delisting procedure, as we recommend immediately below.

Other issues concern the geographic scope of the delisting as well as whether webmasters of the original information need to be informed. In the first case it has been argued that an EU court decision is applicable only in the EU, unless it was granted global scope developing an extraterritoriality effect.[60] The Article 29 Working Party on the other hand asked for global delisting, specifically affecting the domain.com[61] and CNIL already threatens to take action on the same basis. However, the authors believe that delisting should be geographically restricted. On top of an unwanted (or, at least, undiscussed) extraterritoriality effect of a CJEU decision, which would accentuate Kuner's vision of a clash, one should not forget that the *Google Spain* decision is about ease of access to information. Consequently, if an individual wishes to use a proxy in order to enter a Google search as a non-EU user, then that user is evidently determined and capable of unearthing information that is not deleted but only hidden from easy access. On the other hand, informing the webmasters of a delisting decision could prove useful – with the important note that such notification ought not to be perceived under any circumstances as constituting the 'knowledge' requested by the e-Commerce Directive in order for that same webmaster's potential liability to begin.[62] However, details of implementation do matter: In order to avoid a true international clash, with Europeans being perceived as punishing Google and attempting to force their perceptions on distant countries around the globe, moderation and reasonableness are important to keep in mind.

---

58 The Article 29 WP Opinion, para. 23.

59 See ibid., para. 22.

60 See Google Advisory Council report, no. 5.4.

61 See the Article 29 WP Opinion, para. 20.

62 See Article 14 of the e-Commerce Directive and also Sartor's analysis, G. Sartor, 21 *MJECL* (2014), p. 571 et seq.

Finally, individual redress is important. For delisting applicants, in the event that Google has refused to satisfy them, recourse to at least to their local DPA should be possible (whether recourse to a court is also an option is to be established by local law). The Article 29 Working Party has provided ample assistance to DPAs in this regard,[63] in order to ensure uniform application across the EU. While this issue is therefore resolved, we believe that a course of judicial or other assistance ought to be granted to the general public to challenge Google decisions as well. The public has a right to know. The fact that Google and an applicant agreed to have links on the latter removed ought not to be perceived as final and irrevocable. Space for mistakes also on a positive delisting decision ought to be allowed. The public, regardless of whether a single internet user or user groups, ought to be granted the right to challenge Google's (positive) delisting decisions in front of courts and/or DPAs. This is why it is important to know which individual has succeeded in having links removed, if only by means of a single, uniform text applied by Google in all relevant searches.[64]

§7. CONCLUSIONS

As all other the contributors have noted, *Google Spain* is an important decision of the Court of Justice with far-reaching implications. While the Court has taken care to enforce the Lisbon Treaty's human rights protection in the best possible way, as Hijmans notes, it perhaps has taken less care to examine the repercussions of its decision both on the internet and in (legal) substance, as noted by Wolf and Sartor. Aggravating problems by DPAs requesting to apply the Court's decision in the strictest possible manner further justifies Kuner's prediction of a global clash that needs to be defused by the international community. Notwithstanding any theoretical approach, it is practice that brought the difficulties of the Court's decision in plain light. The enthusiastic use of the delisting right across Europe, with 250,000 applications filed in a single year, quickly brought the limitations of applying the Court's decision to the foreground. This is by no means an easy court decision to satisfy. Automation is probably needed as a necessary evil, if any protection is ever to become effective and meaningful. The risks of such automation would probably be mitigated by more transparency, which was repeatedly requested by many stakeholders from Google. However, courts ought to remain the final arbitrator on both ends of the delisting process, meaning both for the parties concerned and the public. A delisting decision is an important decision not only for the applicant but also for the society it relates to; despite any decision-making applied by what ultimately is a private enterprise, all the parties affected by it ought to be able to seek guidance from the institutions established to perform exactly this task, the competent courts.

63 See particularly Part II of the Article 29 WP Opinion.

64 For the time being, Google uses the text 'Some results may have been removed under data protection law in Europe. Learn more', which the authors believe is adequate.