RSCAS 2015/45
Robert Schuman Centre for Advanced Studies
Florence School of Regulation

The *Google Spain* case:
Part of a harmful trend of jurisdictional overreach

Dan Jerker B. Svantesson

European University Institute
Robert Schuman Centre for Advanced Studies
Florence School of Regulation

The *Google Spain* case:
Part of a harmful trend of jurisdictional overreach

Dan Jerker B. Svantesson

EUI Working Paper **RSCAS** 2015/45

ISSN 1028-3625

Printed in Italy, July 2015
European University Institute
Badia Fiesolana
I – 50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu/RSCAS/Publications/
www.eui.eu
cadmus.eui.eu

Robert Schuman Centre for Advanced Studies

The Robert Schuman Centre for Advanced Studies (RSCAS), created in 1992 and directed by Professor Brigid Laffan, aims to develop inter-disciplinary and comparative research on the major issues facing the process of European integration, European societies and Europe's place in 21st century global politics.

The Centre is home to a large post-doctoral programme and hosts major research programmes, projects and data sets, in addition to a range of working groups and *ad hoc* initiatives. The research agenda is organised around a set of core themes and is continuously evolving, reflecting the changing agenda of European integration, the expanding membership of the European Union, developments in Europe's neighbourhood and the wider world.

Details of the research of the Centre can be found on:
http://www.eui.eu/RSCAS/Research/

Research publications take the form of Working Papers, Policy Papers, and e-books. Most of these are also available on the RSCAS website:
http://www.eui.eu/RSCAS/Publications/

Florence School of Regulation

The Florence School of Regulation (FSR) is a partnership between the Robert Schuman Centre for Advanced Studies (RSCAS) at the European University Institute (EUI), the Council of the European Energy Regulators (CEER) and the Independent Regulators Group (IRG). Moreover, as part of the EUI, the FSR works closely with the European Commission.

The objectives of the FSR are to promote informed discussions on key policy issues, through workshops and seminars, to provide state-of-the-art training for practitioners (from European Commission, National Regulators and private companies), to produce analytical and empirical researches about regulated sectors, to network, and to exchange documents and ideas.

At present, its scope is focused on the regulation of Energy (electricity and gas markets), of Communications & Media, and of Transport.

This series of working papers aims at disseminating the work of scholars and practitioners on current regulatory issues.

For further information
Florence School of Regulation Transport Area
Robert Schuman Centre for Advanced Studies
European University Institute
Via delle Fontanelle 19
I-50014 Fiesole (FI)
Tel.: +39 055 4685 795
Fax: +39 055 4685 755
E-mail: fsr.transport@eui.eu
Web:
www.eui.eu/DepartmentsAndCentres/RobertSchumanCentre/Research/Programmes/FlorenceSchoolRegulation.aspx

Abstract

Few legal decisions have gained greater academic and public scrutiny than has the *Google Spain* case and the facts of this so-called 'right to be forgotten' case are widely known.

As could be expected, the CJEU's decision of 2014 is legally technical and addresses a range of topics. Here, I will focus on those aspects of the judgment, and its (suggested) implementation, that has to do with jurisdiction. Those matters must be viewed in their proper context. To that end, this article places the discussion in the context of: (1) the ongoing European data privacy reform, (2) the considerable development of data privacy laws around the globe and (3) the general trend of jurisdictional overreach.

Having done so, a *Model Code Determining the Geographical Scope of Delisting Under the Right To Be Forgotten* is presented and discussed.

Keywords

Extraterritoriality - Right to be forgotten - Jurisdiction - Data Privacy - Google Spain.

1. Introduction

The Internet is made up of both structured and unstructured data in a sense. However, as a whole the Internet is best viewed as being unstructured and data is largely inaccessible until it is searchable.

The widespread availability of relatively accurate search engines means that the unstructured data that makes up the Internet becomes accessible in a manner it would otherwise not have been. And with this accessibility comes increased data privacy concerns.

The important role played by search engines came under the proverbial microscope in a 2014 decision by the Court of Justice of the European Union (CJEU).[1] Few legal decisions have gained greater academic and public scrutiny than has the *Google Spain* case and the facts of the case are widely known.[2]

When Spanish citizen Mr Mario Costeja González, via a Google search, found links to two, for him unflattering, pages of the Spanish newspaper *La Vanguardia* from 1998, he requested that the newspaper remove the personal information about him contained in the relevant pages. He also requested that Google Spain and Google Inc remove or conceal the personal data relating to him so that the data no longer appeared in the search results and in the links to *La Vanguardia*.

The matter ended up before the Spanish data protection authority Agencia Española de Protección de Datos (AEPD). The AEPD rejected the complaint against La Vanguardia. At the same time, it upheld the complaint against Google.

Google brought the matter before the Spanish National High Court (Audiencia Nacional), and that court referred the matter to the CJEU.

As could be expected, the CJEU's decision is legally technical. Here, I will focus on those aspects of the judgment, and its (suggested) implementation, that has to do with jurisdiction.

2. The relevant context

The judgment in the *Google Spain* case, as well as its implications and the reactions it has received must be viewed in their proper context. Account must be had to at least the following aspects: (1) the ongoing European data privacy reform, (2) the considerable development of data privacy laws around the globe and (3) the general trend of jurisdictional overreach.

2.1 The European data privacy reform[3]

Having introduced its trailblazing data protection Directive in 1995, the EU is now looking to modernise its data privacy law through a Regulation that will harmonise the law across Europe. Several parts of the proposal have been controversial,[4] and progress has been slow since the proposal was first released in January 2012.

---

1 Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (Case C-131/12)

2 For a useful, although for obvious reasons incomplete, list of academic commentary of the *Google Spain* case, see: http://www.cambridge-code.org/googlespain.html.

3 This part is based on: http://theconversation.com/how-europes-data-privacy-reform-could-cost-australian-business-24210. For an insightful analysis of the draft Regulation's approach to the right to be forgotten, see: Giovanni Sartor, The right to be forgotten in the Draft Data Protection Regulation, International Data Privacy Law 5(1) (2015) pp. 64-72.

4 https://theconversation.com/the-internet-will-never-forget-you-if-youre-british-16215

Arguably the most controversial aspect of the proposed Regulation is found in the delineation of the Regulation's geographical scope of application. Yet, there has been surprisingly little attention given to this issue.

While latter versions – of which there has been many – have overcome the problem, the initial 2012 proposal was fatally flawed. It extended the Regulation in such a fashion that it would have given Europeans the right to rely on the Regulation even where they were physically present in non-European countries – the law would have followed the person travelling the world.[5] Thus, e.g. a European citizen entering into a contract in a shop in Sydney Australia would have been able to rely on the EU Regulation in relation to any data collected by the shop in Sydney.

In a March 4 speech, European Commission Vice-President, Viviane Reding, stressed that the proposed Data Protection Regulation "is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world."[6]

This argument does not lack merit. However, the idea that the Regulation's wide reach creates a "fair competition in a globalised world" is questionable. In fact, complying with the complex EU data privacy law is likely to be prohibitively expensive for small and medium sized non-EU businesses interacting on the European market on an irregular basis. The result will be that only large foreign businesses, and foreign businesses that do not care about complying with EU law, will be able to afford to enter the European market.

Improved data privacy protection is to be welcomed, but the problem is one of nuance. The proposed EU data privacy Regulation contains many different types of rules. Some rules are aimed at preventing privacy abuse, and such rules are common in privacy laws around the world. There is, of course, nothing unreasonable about non-European companies wishing to benefit from the European market having to abide by EU law protecting against misuse of personal information.

But other rules are administratively burdensome and require changes to business structures. For example, it seems absurd that a non-European organisation with some limited interaction with EU residents also has to implement potentially costly administrative measures such as appointing a Data Protection Officer. Such rules should only apply to businesses that have a substantial presence on the European market.

The solution is obvious. The EU ought to adopt more sophisticated rules as to when the proposed regulation applies outside the EU so as to avoid this type of all-or-nothing situation. We need to see the EU distinguish between the types of data privacy rules it applies to everyone who deals with EU residents, and those rules that only apply to businesses substantially engaging on the European market.[7]

In light of this type of extraordinary jurisdictional oversteps, it is not surprising that non-Europeans may approach European claims of extraterritoriality in the data privacy setting with a degree of suspicion.

2.2 Data privacy law beyond Europe

Greenleaf has carried out extensive research into data privacy laws around the globe. Through this research he has shown that by mid-2014, 103 States across the world had enacted national data privacy

---

5 Dan Svantesson, Extraterritoriality of data privacy law (Ex Tuto, 2013), at 107-108.

6 http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm

7 Dan Svantesson, *A "layered approach" to the extraterritoriality of data privacy laws*, 3(4) INTERNATIONAL DATA PRIVACY LAW 278-286 (2013).

laws.[8] No less than 50 of those States are non-European. Consequently, soon there will be more non-European States with data protection laws than there are European States with such laws. And in light of this, Greenleaf is of course correct in pointing out that innovation in data privacy law is no longer just coming from Europe.[9]

This is important to remember. Europe has and will have the most advanced data protection law in the world, but that does not mean that all aspects of foreign law are inferior or on a lower level than what we find in Europe. Thus, compliance with EU law does not guarantee compliance with all foreign laws.

Europeans will have to take greater steps to familiarise themselves with data privacy developments outside of Europe. After all, European data privacy law is not alone in its approach to extraterritoriality. In fact, while exceptions can be found (e.g. current Japanese data privacy law), there is a tendency of data privacy laws around the world to adopt an extraterritorial scope so that European businesses doing business e.g. in Australia or Singapore will be bound to abide by Australian and Singaporean data privacy law.[10]

In this context, it is also worth recalling that some non-European data privacy laws make possible the awarding of heavy penalties. For example, Trinidad and Tobago's *Data Protection Act 2011* imposes fines up to 10% of the offending party's annual turnover (s. 69).[11] In light of this, the wisdom of justifying breaches of the law by reference to the obvious enforcement difficulties may be called into question.

All this highlights that any approach to the right to be forgotten adopted by the European Union is likely to be mirrored in other States. It is therefore sensible to evaluate all matters not just from the perspective of how well they fit within the overall European data privacy system, but also from the perspective of how well they will suit Europe if adopted in other States' data privacy laws.

2.3 The general trend of jurisdictional overreach

There is a general trend of jurisdictional overreach, and the CJEU's decision in the *Google Spain* case forms part of, and contributes to, this trend. While examples of this trend abound, I will here restrict myself to two recent illustrative court decisions.

2.3.1 The *Garcia* case[12]

The legal drama[13] that has followed in the wake of the online publication of the film titled 'Innocence of Muslims' may be worthy of being used as the plot for a movie in its own right. And, given a recent judgment by Chief Judge Kozinski in the US 9th Circuit, it would no doubt be best set as a horror movie.

---

8 Greenleaf, G 2014, 'South Korea's innovations in data privacy principles: Asian comparisons', *Computer Law & Security Review*, vol. 30, pp. 492-505, at 493.

9 Greenleaf, G 2014, 'South Korea's innovations in data privacy principles: Asian comparisons', *Computer Law & Security Review*, vol. 30, pp. 492-505, at 493.

10 Svantesson, D 2013, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, Copenhagen.

11 For more information about this Act, see: Edmund D Christo 2013, 'Data Protection in Trinidad and Tobago', *International Data Privacy Law*, vol. 3, no. 3, pp. 202-9.

12 This part is based on: http://blawblaw.se/2014/04/ignorance-or-arrogance-%e2%80%93-a-us-court-claims-the-right-to-regulate-the-internet-world-wide/

13 http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000725

The background to the dispute is rather complex, but put simply, Cindy Lee Garcia was cast in a minor role in a film with the working title 'Desert Warrior.' For the three and a half days of filming she received $500. However, that film never materialised. Instead, Garcia's scene was used in another film – a highly controversial film titled 'Innocence of Muslims'.[14] Garcia first saw this latter film after it was uploaded online. At that time, she discovered that her brief performance had been partially dubbed over so that she appeared to be making a statement offensive to persons of the Muslim faith.

Garcia sought to have the movie taken down by arguing to have a copyrightable interest in her brief performance in the movie. Needless to say, such a claim has a slim prospect of success in most parts of the world, but Chief Judge Kozinski concluded that Garcia does have such a right.[15]

Copyright lawyers will no doubt find the decision highly interesting merely by focusing on Chief Judge Kozinski contentious approach to the copyright issues involved. However, our interest in the case lies elsewhere. The concern in our context is that the Court ordered Google Inc to "take down all copies of 'Innocence of Muslims' from YouTube.com *and from any other platforms under Google's control*, and take all reasonable steps to prevent further uploads of 'Innocence of Muslims' *to those platforms*."[16] (emphasis added)

Given Google's virtually global presence, with various country-specific platforms, the problem is obvious. US copyright law applies in the US, not globally. This fact can scarcely have escaped the Court. Yet, it was not even touched upon by the 9th Circuit on this occasion. Indeed, Chief Judge Kozinski did not even seek to legitimise the approach by putting the court order in terms suggesting that the global take down was necessary to ensure the film was inaccessible in the US.

2.3.2 The *Google Canada* case[17]

In *Equustek Solutions Inc. v. Jack*,[18] the Supreme Court of British Columbia granted an injunction requiring Google to block certain websites worldwide.

Google argued that if the injunction was granted it should be limited to Google.ca, the website designated for Canada, for the reason that no court should make an order that has a reach that extends around the world; after all, what is illegal in state A may be perfectly legal, or even demanded by the law, in state B. However, the Court stated that:

> "[A]lthough Google has a website for each country to which searches made within that country default, users can override that default and access other country's Google websites. For example, even if the defendants' websites were blocked from searches conducted through www.google.ca, Canadian users can go to www.google.co.uk or www.google.fr and obtain results including the defendants' websites. On the record before me *it appears that to be effective, even within Canada, Google must block search results on all of its websites. Furthermore, the defendants' sales originate primarily in other countries, so the Court's process cannot be protected unless the injunction ensures that searchers from any jurisdiction do not find the defendants' websites.*"[19] (emphasis added)

Given the availability of alternative search engines, this argument is difficult to maintain. The fact that one particular search engine blocks certain search results worldwide does not affect the availability of

---

[14] http://bits.blogs.nytimes.com/2014/02/26/federal-court-orders-youtube-to-take-down-controversial-anti-islam-video/

[15] http://cdn.ca9.uscourts.gov/datastore/general/2014/02/28/12-57302_opinion.pdf

[16] https://www.techdirt.com/articles/20140226/12103626359/horrific-appeals-court-ruling-says-actress-has-copyright-interest-innocence-muslims-orders-youtube-to-delete-every-copy.shtml

[17] This part is based on: Svantesson, The Canadian 'Google case' – B.C. imperialism or a legitimate response to a difficult issue? LinkedIn (28 August 2014)

[18] Equustek Solutions Inc. v. Jack (2014) BCSC 1063, http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

[19] Equustek Solutions Inc. v. Jack (2014) BCSC 1063, http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

the content in question – the content is still there, it just cannot be found using that particular search engine. Consequently, the content can still be accessed through the use of an alternative search engine.

But the Court, to its credit, had thought of this as well:

> "While there are other search engines, Google does not contest the plaintiffs' assertion that Google's position as the search engine used for 70-75% of internet searches means the defendants will not be commercially successful if they cannot be found through Google's search services."[20]

With this in mind, the Court concluded that:

> "Google is an innocent bystander but it is unwittingly facilitating the defendants' ongoing breaches of this Court's orders. There is no other practical way for the defendants' website sales to be stopped."[21]

The last sentence in this quote is, of course, incorrect. For example, sales require some form of payment method, so one other practical way for the defendants' website sales to be stopped would be to seek to cut the payment mechanism.

The bigger question is this: if the law fails to prevent certain Internet conduct, is it really reasonable that it places the burden of preventing that conduct on the shoulders of what it describes as 'an innocent bystander'?

The court order has been appealed and leave has been granted.[22]

3. The jurisdictional issues of the *Google Spain* case

There are two jurisdictional matters arising in, and from, the *Google Spain* case. Those matters will be discussed here.

3.1 Jurisdiction over Google Inc?

One of the first matters that needed to be considered in the *Google Spain* case was whether only Google's Spanish subsidiary was caught by the Directive or whether also Google Inc in the US fell within the Directive's scope of application. The problem was summarised by Advocate General Jääskinen in the following terms:

> "Google Inc. is a Californian firm with subsidiaries in various EU Member States. Its European operations are to a certain extent coordinated by its Irish subsidiary. It currently has data centres at least in Belgium and Finland. Information on the exact geographical location of the functions relating to its search engine is not made public. Google claims that no processing of personal data relating to its search engine takes place in Spain. Google Spain acts as commercial representative of Google for its advertising functions. In this capacity is has taken responsibility for the processing of personal data relating to its Spanish advertising customers. Google denies that its search engine performs any operations on the host servers of the source web pages, or that it collects information by means of cookies of non registered users of its search engine.
>
> In this factual context the wording of Article 4(1) of the Directive is not very helpful."[23]

There are numerous examples of globally active Internet intermediaries seeking to avoid the jurisdiction of courts by referring to the particular corporate structure they have adopted. For example,

---

[20] Equustek Solutions Inc. v. Jack (2014) BCSC 1063, http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

[21] Equustek Solutions Inc. v. Jack (2014) BCSC 1063, http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

[22] http://www.courts.gov.bc.ca/jdb-txt/CA/14/02/2014BCCA0295.htm

[23] Opinion of Advocate General Jääskinen in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) (Case C-131/12), paras 62-63.

in *A v. Google New Zealand Ltd.*, Google New Zealand successfully argued that "the plaintiff has the wrong defendant, in that its ultimate parent company, Google Inc. (incorporated and resident in the United States of America), owns and operates the search engine."[24] This argument – which also was made in the *Google Spain* case – does not lack merits. After all, as noted by the Court, the fact that Google New Zealand Ltd. may be able to influence Google Inc. to act in a particular manner cannot be seen to make Google New Zealand Ltd. sufficiently connected to the publication as such. Otherwise, as pointed out by Google New Zealand Ltd., it may be subject to a court order (i.e. to remove the relevant search results) that it simply does not have the power to comply with.

However, it may be that courts increasingly will view with suspicion this type of legal argument. In this context, the Court's reaction is telling when Facebook, in a recent Brazilian case, sought to complicate the proceedings by arguing that Facebook Inc and Facebook Ireland Ltd., located in the United States and Ireland respectively, rather than Facebook Brazil, were the appropriate defendants. The Court expressed the view that (1) this argument was an "outrageous disregard" of Brazilian sovereignty, (2) Facebook is not a sovereign country superior to Brazil, and (3) if Facebook wants to operate in Brazil, it is subject to the Brazilian laws, regardless of where the parent companies are incorporated.[25]

In my view, globally active Internet intermediaries – including search engines – need to abandon this type of short-term tactical, but strategically harmful, behaviour in order to maintain credibility; there is little to be gained by allowing globally active Internet intermediaries to rely on a particular corporate structure to make essentially domestic disputes take on a complicating international dimension.

In addressing this complexity, Advocate General Jääskinen adopted what I elsewhere[26] have termed a 'consequence-focused approach'; that is, rather than restricting himself to a blind adherence to the exact wording of the Directive, he sought to identify the consequences of the various possible interpretations. Thus, he noted that on a literal interpretation of Article 4(1) of the Directive, Google has several establishments on EU territory and that this would exclude the applicability of the equipment condition laid down in Article 4(1)(c) of the Directive.[27] Rather than just accepting this, Advocate General Jääskinen stated that, in his opinion "the Court should approach the question of territorial applicability from the perspective of the business model of internet search engine service providers."[28] Thus:

> "processing of personal data takes place within the context of a controller's establishment if that establishment acts as the bridge for the referencing service to the advertising market of that Member State, even if the technical data processing operations are situated in other Member States or third countries."[29]

The CJEU took the following view:

---

[24] *A v Google New Zealand Ltd* [2012] NZHC 2352, at para 4. See also the Australian case: *Duffy v Google INC & Anor* [2011] SADC 178.

[25] Giancarlo Frosio, *A Brazilian Judge Orders Facebook off Air if It Fails to Remove a Defamatory Discussion*,THE CENTER FOR INTERNET AND SOCIETY (October 7, 2013) http://cyberlaw.stanford.edu/blog/2013/10/brazilian-judge-orders-facebook-air-if-it-fails-remove-defamatory-discussion.

[26] Dan Svantesson, What is "Law", if "the Law" is Not Something That "Is"? A Modest Contribution to a Major Question, 26(3) Ratio Juris 456 (2013).

[27] Opinion of Advocate General Jääskinen in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) (Case C-131/12), para 63.

[28] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)* (Case C-131/12), para 64.

[29] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)* (Case C-131/12), para 67.

> "In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.
>
> In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed."[30]

This is all commendable and this reasoning has since been cited with approval in other parts of the world. For example, in the previously mentioned case of *Equustek Solutions Inc. v. Jack*,[31] the Supreme Court of British Columbia specifically referred to the *Google Spain* case and concluded that "Google's search and advertising services are inextricably linked."[32]

3.2 The geographical scope of the right to be forgotten

Importantly, the CJEU was silent on the geographical scope of the right to be forgotten. Thus, different search engines may now be implementing the decision in different ways when it comes to this aspect. Google's implementation has been described by its Global Privacy Counsel, Peter Fleischer:

> "We do not read the decision by the Court of Justice of the European Union ("CJEU") in the case C-131/12 (the "Decision") as global in reach—it was an application of European law that applies to services offered to Europeans.
>
> [...]
>
> It is our long-established practice to comply with national law by processing removals from search results for the version of search on the national ccTLD. We regularly remove results from country-specific versions of search in this manner, typically based on notice through our user-facing webforms informing us of potential violations under national law. For example, users in Germany may alert us to pages featuring extremist content that violates German law, which we would remove from the google.de search results.
>
> In its decision, the CJEU presented a legal interpretation affecting multiple countries simultaneously. We heard some DPAs and others call for consistency across states in implementing it, and we have therefore decided to respect that effort by extending each removal to all EU/EFTA ccTLDs."[33]

However, the Article 29 Working Party's Guidelines regarding the *Google Spain* decision emphasises that:

> "The ruling sets thus an obligation of results which affects the whole processing operation carried out by the search engine. The adequate implementation of the ruling must be made in such a way that data subjects are effectively protected against the impact of the universal dissemination and accessibility of personal information offered by search engines when searches are made on the basis of the name of individuals.

---

30 Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" - C-131/12, paras 55-56.

31 Equustek Solutions Inc. v. Jack (2014) BCSC 1063, http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

32 Equustek Solutions Inc. v. Jack (2014) BCSC 1063, para 63.

33 Peter Fleischer, 'Response to the Questionnaire addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the "right to be forgotten"', 31 July 2014, https://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/view?pli=1&sle=true.

> Although concrete solutions may vary depending on the internal organization and structure of search engines, de-listing decisions must be implemented in a way that guarantees the effective and complete protection of these rights and that EU law cannot be easily circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com."[34]

Thus, the message is clear; the Article 29 Group wants global blocking so as to ensure that EU law is not "circumvented". The question is, of course, whether blocking on the .com domain will be enough to achieve this. Or does the Article 29 Group actually intend search engines to impose delisting also for non-European country domains?

Perhaps the Article 29 Group's wording gives us some hints. After all, it emphasises that: "In practice, this means that in any case de-listing should also be effective on *all relevant domains*, including .com." (emphasis added) If the intention was that delisting should apply to *all* domains, there would be no need for the word "relevant".[35] This suggests that what the Article 29 Group has in mind is delisting on EU domains and on the .com domain.

On the other hand, the very reasoning behind delisting on the global .com domain is that it is easy for people to use google.com to access content delisted on a country-specific search such as google.es – the Spanish domain. But, if content is delisted also on google.com, will not people who are sufficiently motivated to search for the content simply use another country-specific search such as google.com.au? After all, doing so requires little extra effort.

Will this reasoning then mean that to comply with EU law, search engines need to delist search results all over the world, including on distinctly non-EU domains such as Australia's .com.au?

Given the Article 29 Group's decision to issue Guidelines, it would have been useful if it would have engaged with this topic more thoroughly.

4. Towards a better approach

On 6 February 2015, the *Advisory Council to Google on the Right to be Forgotten* provided its Report.[36] The Advisory Council that included eight invited independent experts, each with considerable experience and expertise, provided recommendations as to criteria for assessing delisting requests as well as input on a selection of procedural matters including the question of the geographical scope for delisting. Before dealing with that latter matter in further detail, some observations may appropriately be made more broadly about the principles presented in the Advisory Council's Report. After all, the geographical scope for delisting must be viewed in the context of what principles guide the delisting decision as such.

---

[34] 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' (2014) WP225, at 9.

[35] While far-fetched, it is of course possible that the word "relevant" here is aimed to clarify that it is the domains belonging to a specific search engine that are referred to. However, that would be an unnecessarily cryptic way to express such delineation.

[36] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015.

4.1 The Advisory Council's principles for delisting

The criteria for assessing delisting requests focused on:

1. The data subject's role in public life;
2. The nature of the information the request relates to,
3. The source of the information as well as the motivation for publishing it; and
4. The time that has lapsed between publishing and the delisting request.

As far as the first of these topics is concerned, the Advisory Council devised a three-category structure in which individuals may be grouped; that is, (1) Individuals with clear roles in public life, (2) Individuals with no discernable role in public life and (3) Individuals with a limited or context-specific role in public life.[37] Delisting request from individuals falling into the second category would obviously be more likely to result in delisting than requests by people falling into the first category. And delisting request from individuals within the third category would be most context sensitive.

While it obviously is possible to envisage more complex categorisations, this aspect of the report ought to be relatively uncontroversial.

Looking at the issue of what types of information normally would create a bias towards delisting, the Advisory Council listed the following seven categories:[38]

1. Information related to an individual's intimate or sex life;
2. Personal financial information;
3. Private contact or identification information;
4. Information deemed sensitive under EU Data Protection law;
5. Private information about minors;
6. Information that is false, makes an inaccurate association or puts the data subject at risk of harm; and
7. Information that may heighten the data subject's privacy interests because it appears in image or video form.

The Advisory Council also listed types of information that typically would be of public interest and therefore biased towards delisting request being denied:[39]

1. Information relevant to political discourse, citizen engagement, or governance;
2. Information relevant to religious or philosophical discourse;
3. Information that relates to public health and consumer protection;
4. Information related to criminal activity;
5. Information that contributes to a debate on a matter of general interest;
6. Information that is factual and true;
7. Information integral to the historical record; and
8. Information integral to scientific inquiry or artistic expression.

Most of this ought to also be uncontroversial. However, it is of course always possible to think of additional types of information that could have been included in the lists. For example, focusing on the

---

[37] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 7-8.

[38] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 9-10.

[39] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 10-13.

list of types of information that normally would justify delisting, one may perhaps have expected to see reference to, for example, the following four types of information:

1. Information that is defamatory;
2. Information that amounts to a breach of confidentiality;
3. Information that expresses a threat of physical harm to, or incites violence directed at, the person seeking delisting; and
4. Information that amounts to bullying and harassment.

Turning to the relevance of the source of the information as well as the motivation for publishing it, the Advisory Council expressed the view that:

> "Information that is published by or with the consent of the data subject himself or herself will weigh against delisting. This is especially true in cases where the data subject can remove the information with relative ease directly from the original source webpage, for example by deleting his or her own post on a social network."[40] (footnote omitted)

On the topic of the possibility of seeking deletion of the original content, the Article 29 Group noted that:

> "Individuals are not obliged to contact the original site, either previously or simultaneously, in order to exercise their rights towards the search engines. There are two different processing operations, with differentiated legitimacy grounds and also with different impacts on the individual's rights and interests."[41]

This is of course correct *de lege lata*. However, not least given the ongoing reform of EU data privacy law, we may benefit from pausing to consider this matter *de lege ferenda*. In my view, the matter of whether the data subject is in a position to have the original content removed or not should be given greater attention.

If the data subject is in a position to have the original content removed, then we must question what is gained by allowing a delisting request aimed at the search engine instead. Indeed, one could go as far as to say that data subjects typically should seek the removal of the original content prior to lodging a delisting request with search engines. The very fact that there are multiple search engines makes the removal of the original content, where removal is justified, a more sensible and clearly more efficient option.

In situations where the data subject is not in a position to have the original content removed, we should ask why that is so before we can make an assessment of how this position impacts the right to delisting.

Where removal of the original content is prevented by law – i.e. where the holder of the original content can point to a legal reason why it does not have to remove the content, or indeed, a legal reason why it is not entitled to remove the content – the situation should *prima facie* also favour the denial of a delisting request (especially in the latter situation). However, where the removal of the original content is prevented by practical considerations such as the host being located overseas and refusing to cooperate, the data subject's lacking ability to get the original content removed favours the delisting request being upheld.

In discussing the impact of the time that has lapsed between publishing and the delisting request, the Advisory Council observed how:

---

[40] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 13.

[41] 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' (2014) WP225, at 6.

> "The ruling refers to the notion that information may at one point be relevant but, as circumstances change, the relevance of that information may fade. This criterion carries heavier weight if the data subject's role in public life is limited or has changed, but time may be a relevant criterion even when a data subject's role in public life has not changed. There are types of information for which the time criterion may not be relevant to a delisting decision—for example information relating to issues of profound public importance, such as crimes against humanity.
>
> This criterion will be particularly relevant for criminal issues. The severity of a crime and the time passed may together favor delisting, such as in the case of a minor crime committed many years in the past. It could also suggest an ongoing public interest in the information—for example if a data subject has committed fraud and may potentially be in new positions of trust, or if a data subject has committed a crime of sexual violence and could possibly seek a job as a teacher or a profession of public trust that involves entering private homes."[42] (footnotes omitted)

Aspects of this deserve greater attention than is given in the Report and a revised set of recommendations could more directly address the fluid and changeable relevance of specific information. Content may be seen to be outdated and irrelevant on one date only to become highly relevant again at a later date. For example, information about a person's criminal conduct may be seen to be outdated after a served jail term. But information about the initial crime may become relevant again at a later date if that criminal reoffends. In other words, the relevance of information is not static – it is constantly changing and is always dependent on context.

The question is then who will seek to have the original content – content that has been delisted – re-listed where it regains currency? The criminal will of course not do so, and the search engines will not do so as they may not even be aware of the renewed relevance of the originally delisted search results.

4.2 The Advisory Council's approach to the geographical scope for delisting

As noted above, the Article 29 Group's Guidelines emphasise the need for an implementation that caters for effective and complete protection so that EU law cannot be easily circumvented. This, reasoned the Article 29 Group, requires de-listing on all relevant domains, including .com. Some problems with this have already been highlighted.

The Advisory Council concluded that: "Given concerns of proportionality and practical effectiveness, [...] removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling at this stage."[43] This approach – contrary as it is to the Article 29 Group's Guidelines – was motivated by the following:

- "There is a competing interest on the part of users outside of Europe to access information via a name-based search in accordance with the laws of their country, which may be in conflict with the delistings afforded by the Ruling."[44]
- "There is also a competing interest on the part of users within Europe to access versions of search other than their own."[45]

---

[42] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 14.

[43] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 20. One member of the Advisory Council – Sabine Leutheusser-Schnarrenberger – expressed a dissenting opinion on this matter: "According to my opinion the removal request comprises all domains, and must not be limited to EU-domains. This is the only way to implement the Court's ruling , which implies a complete and effective protection of data subject's rights. The internet is global, the protection of the user's rights must also be global. Any circumvention of these rights must be prevented. Since EU residents are able to research globally the EU is authorized to decide that the search engine has to delete all the links globally." (Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 26-27).

[44] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 19-20.

[45] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 20.

- "It is also unclear whether such measures [technical measures to prevent Internet users in Europe from accessing search results that have been delisted under European law] would be meaningfully more effective than Google's existing model, given the widespread availability of tools to circumvent such blocks."[46]

Further, the Advisory Council noted that:

> "The Council understands that it is a general practice that users in Europe, when typing in www.google.com to their browser, are automatically redirected to a local version of Google's search engine. Google has told us that over 95% of all queries originating in Europe are on local versions of the search engine. Given this background, we believe that delistings applied to the European versions of search will, as a general rule, protect the rights of the data subject adequately in the current state of affairs and technology."[47]

A central question is then the extent to which delisting will affect this statistics. On this point, we can usefully connect to two other matters discussed in the Advisory Council's Report; that is, (1) transparency, and (2) whether or not those whose content gets delisted ought to be informed.

As to the relevant transparency issues, the Advisory Council noted that:

> "The issue of transparency concerns four related but distinguished aspects: (1) transparency toward the public about the completeness of a name search; (2) transparency toward the public about individual decisions; (3) transparency toward the public about anonymised statistics and general policy of the search engine; and (4) transparency toward a data subject about reasons for denying his or her request."[48]

The interesting part in our context here are points 1 and 2 on which the Advisory Council noted the following:

> "With regard to (1) and (2), in general it is our view that the decision to provide notice to users that search results may have been subject to a delisting is ultimately for the search engine to make, as long as data subjects' rights are not compromised. In other words, notice should generally not reveal the fact that a particular data subject has requested a delisting."[49] (footnote omitted)

In the context of whether or not those whose content gets delisted ought to be informed, the Advisory Council noted that:

> "In our public consultations, representatives from the media expressed concerns that delisting decisions could severely impact their rights and interests. To mitigate these potential harms, the aforementioned representatives suggested that they should receive notice of any delistings applied to information they had published.
>
> However, some experts argued that notifying webmasters may adversely impact the data subject's privacy rights if the webmaster is able to discern either from the notice itself or indirectly who the requesting data subject is.
>
> The Council also received conflicting input about the legal basis for such notice. Given the valid concerns raised by online publishers, we advise that, as a good practice, the search engine should notify the publishers to the extent allowed by law."[50] (footnotes omitted)

All of this is, of course, highly relevant for the likelihood that people will start using the .com domain, or indeed country domains of non-European States, to access content they expect is delisted in the

---

[46] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 20. See further: Dan Svantesson, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, SCRIPT-ed 11(2) (2014) pp. 153-170.

[47] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 19.

[48] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 21.

[49] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 21.

[50] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 17.

European search results. Consequently, great care must be taken when it comes to how search engines provide transparency and the extent to which those whose content gets delisted are informed.

The potential for change in user patterns also highlights the wisdom of the Advisory Council limiting its statement as to the geographical scope to "the current state of affairs and technology" "at this stage".

Finally,it is possible to read the Advisory Council's call for delisting to be limited to the European domains as merely expressing a general rule. Indeed this message is made explicit in the second of the five paragraphs dealing with the geographical scope in the Advisory Council's Report:

> "Given this background, we believe that delistings applied to the European versions of search will, *as a general rule*, protect the rights of the data subject adequately in the current state of affairs and technology."[51] (emphasis added)

However, when the reader reaches the fifth and final paragraph relating to the issue of the geographical scope, that messages has been dropped:

> "Given concerns of proportionality and practical effectiveness, [...] removal from nationally directed versions of Google's search services within the EU is the appropriate means to implement the Ruling at this stage."[52]

This creates an unnecessary ambiguity since many readers presumably will read the last paragraph – the paragraph that follows from the full discussion of the matter – as the Advisory Council's final conclusion on the matter, and thereby will overlook the important caveat included in the second paragraph.

4.3 The necessity of a consequence-focused approach also in this context

Like both he and the Court had done in relation to the scope of Article 4(1) of the Directive (see above), Advocate General Jääskinen adopted the consequence-focused approach more generally in his approach to the case:

> "In the current setting, the broad definitions of personal data, processing of personal data and controller are likely to cover an unprecedently wide range of new factual situations due to technological development. This is so because many, if not most, websites and files that are accessible through them include personal data, such as names of living natural persons. This obliges the Court to apply a rule of reason, in other words, the principle of proportionality, in interpreting the scope of the Directive in order to avoid unreasonable and excessive legal consequences. This moderate approach was applied by the Court already in Lindqvist, where it rejected an interpretation which could have lead to an unreasonably wide scope of application of Article 25 of the Directive on transfer of personal data to third countries in the context of the internet.

Hence, in the present case it will be necessary to strike a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and internet users at large."[53] (footnote omitted)

---

[51] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 19.

[52] Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 20. One member of the Advisory Council – Sabine Leutheusser-Schnarrenberger – expressed a dissenting opinion on this matter: "According to my opinion the removal request comprises all domains, and must not be limited to EU-domains. This is the only way to implement the Court's ruling , which implies a complete and effective protection of data subject's rights. The internet is global, the protection of the user's rights must also be global. Any circumvention of these rights must be prevented. Since EU residents are able to research globally the EU is authorized to decide that the search engine has to delete all the links globally." (Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 26-27).

[53] Opinion of Advocate General Jääskinen in Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) (Case C-131/12), paras 30-31.

The importance of this observation cannot be emphasised enough. The reality is that the legal framework we are working with here is structured in such a manner that its application to some forms of Internet activities can only be *either* sensible *or* coherent – it just cannot be both. In such a situation, people's underlying articulated or unarticulated jurisprudential leanings will be determinative. Thus, my tendency to agree with the approach articulated by Advocate General Jääskinen on this topic admittedly stems from my particular view of what "law" is.[54]

At any rate, those, like the Article 29 Group, who attempt to impose global blocking based on local European values cannot be viewed in isolation. As was made clear by reference to the US *Garcia* case, and the *Google Canada* case, they have their counterparts in other States.

Furthermore, their attitude may be seen as natural and may even be viewed as necessary by some; after all, the most effective way to ensure that content cannot be accessed is through global blocking. But the problems caused by this attitude abound.

Most importantly, if our standard position is global blocking based on our local laws, we can hardly object to other States doing the same. So when repressive dictatorships seek global removal of content offensive to their laws, supporters of the *Garcia* case, the *Google Canada* case and the Article 29 Group's Guidelines can hardly protest based on the effect such removal may have in open tolerant and democratic States.[55]

The reality is that the trend of courts demanding global blocking based on local laws will inevitably lead to the destruction of a common resource – the Internet as we know it. And no matter what the European Commission is trying to tell us, this is not a myth.[56] After all, what would be left online if anything that may be unlawful somewhere in the world was removed globally?

Addressing this trend may be both the biggest, and the most important, challenge for Internet regulation today. And the solution we adopt must fit all legal systems, not just trusted European legal systems.

Given the above, I maintain the position I expressed elsewhere[57] that violations of local laws cannot as default be met by global blocking. This is of particular importance given that not only EU citizens may seek to rely on the *Google Spain* judgment to have content delisted. Consider, for example, the following insightful example provided by Kuner:

> "For example, it seems that under the judgment there would be no reason why a Chinese citizen in China who uses a US-based Internet search engine with a subsidiary in the EU could not assert the right affirmed in the judgment against the EU subsidiary with regard to results generated by the search engine. Since only the US entity running the search engine would have the power to amend the search results, in effect the Chinese individual would be using EU data protection law as a vehicle to bring a claim against the US entity. The judgment therefore potentially applies EU data protection law to the entire Internet, a situation that was not foreseen when the Directive was enacted. This could lead to forum shopping and 'right to suppression tourism' by individuals with no connection to the EU other than the fact that they use Internet services that are also accessible there. Even if the judgment is likely to be interpreted in practice more restrictively than this, such

---

54 Dan Svantesson, What is "Law", if "the Law" is Not Something That "Is"? A Modest Contribution to a Major Question, 26(3) Ratio Juris 456 (2013).

55 On this the Council noted how: "The Council has concerns about the precedent set by such measures, particularly if repressive regimes point to such a precedent in an effort to "lock" their users into heavily censored versions of search results." (Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 20).

56 European Commission, Myth-Busting: The Court of Justice of the EU and the "Right to be Forgotten" http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtbf_mythbusting_en.pdf.

57 Dan Svantesson, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, SCRIPT-ed 11(2) (2014) pp. 153-170.

> broad application cannot be excluded based on the wording of the judgment."[58] (footnotes omitted)

In the end, we must also link the discussion about the geographical scope for delisting to the more general discussion of what a right to be forgotten actually ought to achieve. A full discussion of that latter topic is beyond the scope of this paper. However, on the most fundamental level it is my impression that the right to be forgotten, at least as articulated in the *Google Spain* case, aims at what we can call a 'first impression protection' rather than a more absolute protection. After all, an absolute protection cannot be achieved where the original content remains online accessible for anyone who knows enough about the content to formulate a successful search string that does not include the object's personal name, or indeed anyone who happens to come across the content when browsing the Internet.

And if the right as such is not absolute, why should the implementation of the judgment be absolute in a geographical sense? Given the undisputed fact that an overwhelming majority of people use their local search engine version, it seems a 'first impression protection' may be achieved by delisting limited to EU domains. And if anything beyond that is desired, it is, as highlighted above, not enough to extend the delisting to the .com domain. Rather, should the implementation of the judgment be absolute in a geographical sense, it must extend to all domains, of all search engines, including the country domains of non-European states. This latter option comes with obvious and severe consequences.[59]

4.4 Seeing the nuances in a complex grey zone

Elsewhere[60] I have acknowledged that, while global blocking based on the violation of local laws should not be the general default position, global blocking may well be justified in some instances. Thus, the question of the appropriate geographical scope of delisting under the right to be forgotten need not be the same for all requests for delisting. For some request, the delisting ought to be local, in other the delisting could go beyond local covering several States, or even be global. Consequently, we need a more nuanced approach than those articulated by the Article 29 Group, Google and the Advisory Council – as astutely noted by Powles "If delisting is determined on a case-by-case basis, surely the remedy can be too."[61]

In September 2014, I articulated the following four principles that could guide us in deciding whether or not to block Internet content on a global scale based on local laws:

> ***Principle 1:*** *The extent to which a court order in one country should force the blocking/removal of content beyond that country must depend on the type of legal action that produced the relevant court order.*
>
> ***Principle 2:*** *Generally, orders requiring global blocking/removal should only be awarded against the party who provided the content, not parties that merely act as intermediaries in relation to that content. And such orders should only be awarded by the courts at the defendant's place of domicile.*

---

[58] Christopher Kuner, The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines (LSE Law, Society and Economy Working Papers 3/2015) www.lse.ac.uk/collections/law/wps/wps.htm, at 11-12.

[59] See e.g. Dan Svantesson, Between a rock and a hard place – an international law perspective of the difficult position of globally active Internet intermediaries, Computer Law & Security Review 30 (2014) pp. 348-356 and Dan Svantesson, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, SCRIPT-ed 11(2) (2014) pp. 153-170.

[60] Dan Svantesson, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, SCRIPT-ed 11(2) (2014) pp. 153-170.

[61] http://www.slate.com/articles/technology/future_tense/2015/02/google_and_the_right_to_be_forgotten_should_delisting_be_global_or_local.html.

> ***Principle 3:*** *Exceptions to Principle 2 should be made in relation to particularly serious content such as child pornography materials.*
>
> ***Principle 4:*** *In relation to rights limited to the territory of a specific country, whether based on registration or not, courts should not order blocking/removal beyond that country.*[62]

By referring to child pornography materials as an example of "particularly serious content", I do not mean to suggest that only materials as grave as that can justify global blocking, or delisting as in the case of the current context. Also other types of material may indeed justify a global blocking; one such example being so-called revenge porn.

At least when it comes to major Internet companies, I suspect we are starting to see a trend of stronger, or at least clearer, corporate social responsibility in relation to what content is blocked. Focusing on revenge porn, for example, Twitter now makes clear that: "You may not post intimate photos or videos that were taken or distributed without the subject's consent."[63] And on March 16, 2015, Facebook announced new "Community Standards" to govern the conduct of its 1.39 billion users. Also this policy specifically addresses revenge porn:

> "To protect victims and survivors, we also remove photographs or videos depicting incidents of sexual violence and images shared in revenge or without permissions from the people in the images.
>
> Our definition of sexual exploitation includes solicitation of sexual material, any sexual content involving minors, threats to share intimate images, and offers of sexual services. Where appropriate, we refer this content to law enforcement."[64]

This is an important step, and follows a recent announcement by social media site Reddit that it has banned non-consensual nude photos shared on its site.[65]

In assessing the true value of these initiatives, we end up in the now classic topic of self-regulations vs. legal regulation. In this context we can usefully pause to consider how a member of the Advisory Council – Frank La Rue – in his dissenting opinion expressed the following:

> "I must remind that the protection of Human Rights is a responsibility of the State, and in the cases where there can be limitations to the exercise of a right to prevent harm or violation of other rights or a superior common interest of society, it is the State that must make the decision. Therefore I believe it should be a State authority that establishes the criteria and procedures for protection of privacy and data and not simply transferred to a private commercial entity."[66]

This is an important point. Private companies operating search engines are unsuitable, and often unwilling, filters for what is 'good taste' for the Internet. Perhaps the better approach would be for a specific governmental department to receive and evaluate delisting requests and then notify the search engines of their decisions. Such a model would also have the advantage of avoiding complainants having to turn to multiple search engines in relation to the same content.

In any case, in a highly interesting paper dealing specifically with the extraterritorial reach of the right to be forgotten, Van Alsenoy and Koekkoek have proposed "four factors to determine whether a State can 'reasonably' demand global implementation"[67]:

1. How would global delisting impact the interests of residents of other states?

---

62 Dan Svantesson, Delineating the Reach of Internet Intermediaries' Content Blocking – 'ccTLD Blocking', 'Strict Geo-location Blocking', or a 'Country Lens Approach'?, SCRIPT-ed 11(2) (2014) pp. 153-170.

63 https://support.twitter.com/articles/18311-the-twitter-rules

64 https://www.facebook.com/communitystandards#

65 https://theconversation.com/reddit-tackles-revenge-porn-and-celebrity-nudes-38112

66 Advisory Council to Google on the Right to be Forgotten, Report of 6 February 2015, at 29.

67 Van Alsenoy, Brendan and Koekkoek, Marieke, The Extra-Territorial Reach of the EU's 'Right to Be Forgotten' (January 19, 2015). ICRI Research Paper 20. Available at SSRN: http://ssrn.com/abstract=2551838, at 27.

2. What is the likelihood of adverse impact if delisting is confined to local search results?
3. To what extent is the norm to be enforced harmonised across other States?
4. What factors create a territorial *nexi* to the forum State?[68]

These factors are helpful indeed, but like the four principles I had advocated they could perhaps be complimented by a clearer focus on the types of content is in question. And here we can usefully reconnect with the useful recommendations made by the Advisory Council.

Further, it is also necessary to flesh out the issue of what types of connections are required to create a sufficient nexi to the forum State. In contrast to Van Alsenoy and Koekkoek, I prefer to stay clear of a focus on territory in this context. For reasons I have outlined elsewhere,[69] I advocate a departure from our traditional focus on the territoriality principle in favour of, what I see as a more contemporary approach, focused on "substantial connections" and "legitimate interests".

Combining all this then, the following model could be advanced:

> **Model Code Determining the Geographical Scope of Delisting Under the Right To Be Forgotten**
>
> *Article 1 – General provision*
>
> Where a request for delisting has been approved, its implementation should, apart from what appears in Articles 2-4, be limited to EU domains.
>
> *Article 2 – Harmonised laws*
>
> Where a delisting request has been approved for the EU domains, and the request includes evidence that delisting could be ordered under the laws of a non-EU State in relation to that State's domain, the delisting should be extended to such a domain.
>
> *Article 3 – Particularly serious content*
>
> Where a delisting request has been approved for the EU domains and the request relates to particularly serious content, the delisting should be extended globally.[70]
>
> What amounts to "particularly serious content" is context-specific and no exhaustive general list can be devised. However, the following categories are examples of types of content that typically may justify delisting with global effect:
>
> a) Sexual content involving minors;
> b) Non-consensually disclosed sexual content (revenge porn);
> c) Content that is clearly defamatory, having regard to all relevant considerations including the person's position in society;
> d) Content that expresses a threat of physical harm to, or incites violence directed at, the person seeking delisting; and
> e) Confidential details the disclosure of which exposes the person seeking delisting to a serious risk of fraud or theft.
>
> *Article 4 – Other situations justifying delisting beyond the EU domains*
>
> Where a delisting request has been approved for the EU domains, and:
>
> a) it has a substantial connection to at least one member state of the EU;

---

[68] Van Alsenoy, Brendan and Koekkoek, Marieke, The Extra-Territorial Reach of the EU's 'Right to Be Forgotten' (January 19, 2015). ICRI Research Paper 20. Available at SSRN: http://ssrn.com/abstract=2551838, at 25-26.

[69] Dan Svantesson, Do we need new laws for the age of cloud computing? (3 Feb. 2015) https://agenda.weforum.org/people/dan-jerker-b-svantesson/.

[70] Alternatively this Article could be given a somewhat broader wording, such as: "Where a delisting request has been approved for the EU domains and the request relates to particularly serious content, the delisting should be extended globally, or as widely as is appropriate in the circumstances.".

b) there is a legitimate interest in applying that member state's law to the request;

c) delisting on non-EU domains is unlikely to impacts the interests of residents of those other states;

d) there is a high likelihood of adverse impact if delisting is confined to local search results, for example due to the content being such that persons are likely to seek it out via non-EU domains; and

e) it is shown that attempts at having the original content removed or blocked either have failed, or are highly likely to fail, due to lacking cooperation from the content host,

delisting should be extended beyond the EU domains, potentially globally, as appropriate.

In assessing whether a delisting request has a substantial connection to a member state of the EU, regard shall be had to factors such as:

a) The nationality, habitual residence and centre of interest of the requesting party;

b) The nationality, habitual residence and centre of interest of the publisher of the original content; and

c) The geographical scope of interest of the content.

The same factors should form part of the assessment of whether delisting going beyond the EU domains impacts the interests of residents of other states.

Article 1 should require little explanation. It sets down the general rules that delisting should be limited to the EU domains apart from where the issue at hand can be fitted into one of the exceptions outlined in Articles 2-4. The only thing to note here is that, should the model be framed in more general terms so that it can be applied also outside of the EU, we would obviously need to remove the reference to the ”EU domains” and instead refer to e.g. ”the local domain”.

The aim of Article 2 is to create a one-stop shop allowing data subjects to request delisting across all domains governed by the same, or sufficiently similar, laws. This would of course improve efficiency both for the data subject and the search engines in minimising overlapping requests. And indeed, Google's decision to extend delisting to all EU domains can be viewed as an example of this principle already being applied.

Admittedly, there may, however, well be instances where it is difficult to assess whether the relevant laws are similar enough to justify the application of Article 2. With that potential fir complications in mind, it may be that Article two requires some fine-tuning, or that it indeed should be left out of the Model Code.

As is made explicit in Article 3, the complex part of its application relates to how we should define what amounts to ”particularly serious content”. The Article does canvass some examples, but more generally, one matter that will be helpful in determining whether certain content fits into the category of “particularly serious content” or not, is whether the nature of the content is such that a reasonable person would legitimately be concerned or offended about a random third person viewing that content. For example, the availability of the sort of financial information at issue in the *Google Spain* case may only legitimately trouble a reasonable person where it is accessed by, either a person who knows the data subject or may enter into dealings or contact with the data subject. In contrast, a reasonable person may legitimately feel uncomfortable about revenge porn content depicting the sexual activities of the data subject even where that content is accessed by a random third person. Similarly, the potential harm that may stem from confidential details that exposes the data subject to a serious risk of fraud or theft may, of course, be a legitemate concern also where that content is accessed by a random third person.

This test may also be particularly effective in assessing whether specific defamatory content is so serious as to fall into the category of ”particularly serious content”; after all, some types of defamatory content is only of concern where it is accessed by a third person with a connection to the data subject. Other type of defamatory content – such as an untrue claim that a particular person is a convicted war

criminal – may legitimately be a concern even where it is only accessed by random third persons. Finally as to Article 3, it may be that instead of only referring to global delisting, the Article should refer to delisting as widely as is appropriate in the circumstances.

Article 4 attempts to capture all other situations in which it may be legitimate to extend delisting beyond the local domain(s). In trying to strike an appropriate balance that usefully can be applied across a diverse range of fact scenarios, it is unavoidably the most complex Article in the Model Code.

Rather than focusing on territorial connecting factors, Article four focuses on whether there is a substantial connection and a legitemate interest. And indeed, also the Article 29 Group acknowledges that, on a practical level, the European interest is limited to data subjects with a strong connection to Europe:

> "Article 8 of the EU Charter of Fundamental Rights, to which the ruling explicitly refers in a number of paragraphs, recognizes the right to data protection to "everyone". In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State."[71]

Article 4 then draws, and expands, upon some principles articulated by Van Alsenoy and Koekkoek and also adds a requirement relating to the potential removal of the original content. This last requirement seems justified given the discussion above of the relevance of the original content.

5. Concluding remarks[72]

It is both amazing and amusing how a well chosen expression may capture our imagination. 'Cloud computing', 'big data' and the 'right to be forgotten' are all examples of phenomena that existed prior to, but came to life through, the catchy labels we attached to them. Am I the only one worried by this? Is there not something odd about the idea that the focus of legal, and other, researchers is so strongly guided by something as flimsy as catchy labels?

The 'right to be forgotten' has attracted considerable attention for some years now both in legal circles and in media. And as is well-known, much, perhaps too much, of the focus of the undergoing reform work of the EU data privacy framework has been devoted to this right.

The relevant legal landscape in Europe has been largely unaltered since the Data Protection Directive (Directive 95/46[73]) was introduced in the mid-90s. So the thought that the current debate influenced the CJEU's willingness to embrace a right to be forgotten in *Google Spain SL* (Case C-131/12) is difficult to escape.

At any rate, even if the Court spoke expressly about a right to be forgotten, it seems to me that, that was not what was delivered in the judgment. The court order is not focused on any such right. If it was, it would have required the original publisher (*La Vanguardia*) to remove the content as well, but it did not.

The real effect of the judgment is to impose a 'duty to be forgetful' onto certain Internet actors – in this case search engines, or indeed, one particular search engine.

---

71 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' (2014) WP225, at 8.

72 This section partly draws upon: http://blawblaw.se/2014/08/%e2%80%98right-to-be-forgotten%e2%80%99-v-%e2%80%98duty-to-be-forgetful%e2%80%99-and-the-importance-of-correct-labelling/

73 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

So does this matter? I think it does. First of all, politically, it is of course always easier to 'sell' a right than it is to sell a duty. And second, as was referred to more generally above, the labels guide, or even control, our thinking to a large extent.

In the text above, I have sought to draw attention to the jurisdictional issues that arose in, and stem from, the *Google Spain* decision. More specifically, I first addressed the question of whether the Directive applies to the conduct of Google Inc based in the US. It was shown that both the Advocate General and the Court sensibly adopted what we can call a consequence-focused approach in disposing of this issue.

The second jurisdictional issue – that of the geographical scope of the right to be forgotten – needed to be dealt with in more detail. After all, this matter goes more directly to the future implications of the judgment. And just how controversial this issue is can be seen with great clarity in the fact that while the Article 29 Group's Guidelines on the implementation of the judgment specifically calls for delisting to go beyond the EU domains, recommendations of the Advisory Council to Google on the Right to be Forgotten specifically calls for delistings to be limited to the EU domains, at least at this stage.

I asserted that the question of the geographical reach of the right to be forgotten is context specific and that the solution consequently needs to be more nuanced than these two extremes – and also here should we adopt a consequence-focused approach.

To that end, I proposed a *Model Code Determining the Geographical Scope of Delisting Under the Right To Be Forgotten*. The Model Code draws upon my earlier research on blocking issues, the findings made in this paper, some of the classifications made in the Advisory Council's report and the four factors to determine whether a State can 'reasonably' demand global implementation presented by Van Alsenoy and Koekkoek.

There can be no doubt that the road ahead for the right to be forgotten – or rather the duty to be forgetful – is going to be long and continue to be controversial. However, given the attention it has generated, it represents a good test case for ironing out some of the jurisdictional issues that have plagued the Internet since it started crossing borders. Thus, there is every reason to continue the interesting debate that the controversial *Google Spain* case has generated to date.

Author contacts:

Dan Jerker B. Svantesson

Centre for Commercial Law, Faculty of Law, Bond University

Gold Coast, Queensland, 4229

Australia

CRICOS Provider Code: 00017B

Email: Dan_Svantesson@bond.edu.au