Limitless Borderless Forgetfulness? Limiting the Geographical Reach of the ‘Right to be Forgotten’

Dan Jerker B Svantesson

Abstract

In Google Spain, the Court of Justice of the European Union ruled that, in certain circumstances, the operator of a search engine is obliged to remove search results from the list of results displayed following a search made on the basis of a person’s name.

In respect of implementation of this ‘right to be forgotten’ — or more accurately ‘right to delisting’ — one of the most important issues relates to the geographical scope of the delisting: that is, once it is decided that certain search results should be delisted, what is the appropriate geographical scope of the delisting? Google is currently only delisting in relation to EU domains such as .es, .nl and .de. However, in sharp contrast, the EU’s Article 29 Working Party on data protection wants global blocking so as to ensure that EU law is not ‘circumvented’.

This article canvasses the contours of this issue and attempts to advance its resolution by proposing a Model Code for Determining the Geographical Scope of Delisting Under the Right to Delisting. While the Model is presented in the EU context, it can easily be transplanted into other jurisdictions as well.

Keywords: Data privacy; jurisdiction extraterritoriality; right to be forgotten; right to delisting

1. Introduction

The important role played by Internet search engines came under the proverbial microscope in a 2014 decision by the Court of Justice of the European Union (CJEU). Few recent legal decisions have gained greater academic and public scrutiny than has

---

*This article was completed during the author's time as a Visiting Researcher at the Norwegian Research Center for Computers and Law at the University of Oslo. It is based on the author's presentations at Florence School of Regulation Communications and Media: Annual Scientific Seminar on the Economics, Law and Policy of Communications and Media 2015 (Florence 27-28 March 2015), at the Experts Seminar on the Right to be Forgotten at the European University Institute (Florence 30 March 2015) and at the Jon Bing Memorial Seminar (Oslo 30 April 2015). It builds on and refines the author's 2015 contribution in the Florence School of Regulation Communications and Media Working Papers Series entitled 'The Google Spain case: Part of a harmful trend of jurisdictional overreach'.

**Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia); Visiting Professor, Faculty of Law, Masaryk University (Czech Republic); researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council.

1 Case C-131/12 Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González, ECR report forthcoming (hereinafter 'Google Spain case').
the *Google Spain* case, and the facts of the case are widely known.² Put briefly, 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.

The CJEU decided that the activity of a search engine should be classified as ‘processing of personal data’ when the search results contain personal data,³ and that the operator of the search engine must be regarded as the ‘controller’ in respect of that processing.⁴ From this followed that, in certain circumstances, the operator of a search engine is obliged to remove certain search results from the list of results displayed following a search made on the basis of a person’s name.⁵ This requirement needs to be met also in a case where that name or information is not erased beforehand or simultaneously from the original web pages, and even, as the case may be, when its publication in itself on those pages is lawful.⁶ At the same time, the CJEU ruled that the request does not need to be met where it appears that the interference with a person’s fundamental rights is justified by the general public’s preponderant interest in having access to the information in question (for example, where the data subject occupies a certain role in public life).⁷

It is this right articulated by the CJEU — the right to request that a search engine remove certain search results from the list of results displayed following a search made on the basis of a person’s name — that I throughout mainly refer to as the ‘right to delisting’.⁸ Others — probably a majority — refer to this right as the ‘right to be forgotten’, while yet others mean something slightly different when they speak of a ‘right to be forgotten’.⁹ Then there is the term ‘right to erasure’ commonly used in the context of Article 17 of the proposed General Data Protection Regulation.¹⁰ I do not here intend to spend time in this definitional quagmire. This article quite simply deals with the right

---

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> accessed 14 September 2015.
³ *Google Spain SL* (n 1) at [100].
⁴ ibid.
⁵ ibid.
⁶ ibid.
⁷ ibid.
⁹ For a useful discussion of the diverse terminology, see eg Meg Leta Ambrose and Jef Ausloos, ‘The Right to Be Forgotten Across the Pond’ (2013) 3 *Journal of Information Policy* 1.
¹⁰ See eg Ambrose and Ausloos (n 9).
articulated by the CJEU in the *Google Spain* case, whatever label may best be attached to it.

There is a wealth of good papers discussing and analysing the decision in general.\textsuperscript{11} However, comparatively little attention has been given to the jurisdictional aspects of the judgment’s implementation;\textsuperscript{12} that is, once it is decided that certain search results should be delisted, what is the appropriate geographical scope of the delisting? Most importantly, should the delisting be limited to the EU, or can it go beyond the EU? Here, I will focus on those questions; in doing so I restrict myself to the EU context even though it is to be noted that there is also a clear and increasing appetite for implementing the right to delisting in states outside of Europe.\textsuperscript{13}

First, I discuss the different attitudes that have emerged as to the geographical scope of the right to be forgotten. Then, I seek to identify an alternative approach that better caters for the interests involved. Finally, I outline some concluding observations.

### 2. The Geographical Scope of the Right to be Forgotten

Notably, 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 [Data Protection Authorities] 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.14

In sharp contrast, the Article 29 Working Party’s15 Guidelines16 regarding the Google Spain decision emphasise 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.

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

14 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/0BBsyaa68SslT0ErUFyOENqR3M/view?pli=1&sl=1true> accessed 14 September 2015. For more on Google’s actual implementation of the decision, refer to its transparency report: ‘European privacy requests for search removals’ <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> accessed 14 September 2015. The reference to ‘ccTLDs’ refers to ‘country code top-level domains’ such as .se, .no or .dk.

15 The Article 29 Data Protection Working Party is composed of representatives of the supervisory authorities of each EU member state, along with representatives of the authorities established for EU institutions and a representative of the European Commission. It was established pursuant to Article 29 of Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data Protection Directive). It has advisory status only. See further European Commission, Article 29 Working Party (11 September 2015) <http://ec.europa.eu/justice/data-protection/article-29/index_en.htm> accessed 14 September 2015.

16 Art 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” Case C-131/12’ (2014) WP225, 5 (stating that the Guidelines are ‘designed to provide information as to how the DPAs assembled in the Working Party intend to implement the judgment of the CJEU in the case of “Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” (Case C-131/12)’).
de-listing should also be effective on all relevant domains, including .com.17

Thus, the message is clear: the Article 29 Working Party 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 Working Party actually intend search engines to impose delisting also for non-European country domains? Perhaps the Article 29 Working Party’s wording gives us some hints. 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’.18 This suggests that what the Article 29 Working Party 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 currently easy for people to use google.com to access content delisted on a country-specific search such as google.es — the Spanish domain. Yet, if content is delisted also on google.com, will not people who are sufficiently motivated to search for the content simply use another non-EU 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, Japan’s .jp and Colombia’s .co? Given the decision of the Article 29 Working Party to issue Guidelines, it would have been useful if it would have engaged with this topic of fundamental importance more thoroughly.

---

17 ibid 9. This approach has recently been emphasised by the French data protection authority — the Commission Nationale de Informatique et Libertés (CNIL) — in a media release of 12 June 2015 stating, amongst other things, that: ‘CNIL considers that in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing. In this context, the President of the CNIL has put Google on notice to proceed, within a period of fifteen (15) days, to the requested delisting on the whole data processing and thus on all extensions of the search engine.’ CNIL orders Google to apply delisting on all domain names of the search engine’ <http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/> accessed 14 September 2015.

18 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.
3. Towards a Better Approach

3.1. The Advisory Council’s Principles for Delisting

On 6 February 2015, the Advisory Council to Google on the Right to be Forgotten provided its Report.\(^1\) The Advisory Council comprised eight invited independent experts,\(^2\) each with considerable experience and expertise. Its remit was to provide 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 the 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 which principles guide the delisting decision as such.

The criteria for assessing delisting requests focused on:

1) The data subject’s role in public life;
2) The nature of the information to which the request relates;
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.

It is not my ambition to analyse these criteria in any detail. However, as some of the discussions and categorisations provided in the Advisory Council’s report are highly useful and of great significance for the topic of this article, I will make a selection of observations.

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 discernible role in public life; and
3) Individuals with a limited or context-specific role in public life.\(^3\)

As to the definition of ‘a role in public life’, the Article 29 Working Party articulated a useful guiding principle: ‘A good rule of thumb is to try to decide where the public having access to the particular information — made available through a search on the

---


\(^2\) The members of the Advisory Council to Google on the Right to be Forgotten were: Luciano Floridi (Professor of Philosophy and Ethics of Information at the University of Oxford), Sylvie Kauffman (Editorial Director, Le Monde), Lidia Kolucka-Zuk (Director of the Trust for Civil Society in Central and Eastern Europe), Frank La Rue (UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression), Sabine Leutheusser-Schnarrenberger (former Federal Minister of Justice in Germany), José Luis Piñar (Professor of Law at Universidad CEU and former Director of the Spanish Data Protection Agency), Peggy Valcke (Professor of Law at University of Leuven) and Jimmy Wales (Founder and Chair Emeritus, Board of Trustees, Wikimedia Foundation).

\(^3\) Advisory Council (n 19) 7-8.
data subject’s name — would protect them against improper public or professional conduct.\textsuperscript{22}

Delisting requests 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. Furthermore, delisting requests from individuals within the third category would be most context sensitive. While it is obviously 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:\textsuperscript{23}

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 the delisting request being denied:\textsuperscript{24}

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 also to 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 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;

\begin{itemize}
\item[22] Art 29 Data Protection Working Party (n 16) 13.
\item[23] Advisory Council (n 19) 9-10.
\item[24] ibid 10-13.
\end{itemize}
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.\(^{25}\)

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.\(^{26}\) (footnote omitted)

On the topic of the possibility of seeking deletion of the original content, the Article 29 Working Party 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.\(^{27}\)

This is of course correct \textit{de lege lata}. However, not least given the ongoing reform of EU data privacy law, we may benefit from pausing to consider this matter \textit{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 — that is, 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 \textit{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

\(^{25}\) See the reference to 'hate speech, slander, libel, identity theft and stalking' in Art 29 Data Protection Working Party (n 16) 16-18.

\(^{26}\) ibid 13.

\(^{27}\) ibid 6.
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:

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.28 (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. However, 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. Arguably, the concern articulated above falls into the category of ‘theoretical’ or ‘academic’ concerns; after all, where the old news regains currency, good journalists will bring them back into the limelight.29 However, and this is important, it is no doubt possible to envisage fact scenarios in

---

28 Advisory Council (n 19) 14.
29 I am indebted to Jef Ausloos and David Lindsay for their input on this particular point.
which delisted search results regain relevance without investigative journalists taking an interest.

3.2. The Advisory Council’s Approach to the Geographical Scope for Delisting

As noted above, the Article 29 Working Party’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 Working Party, 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.’

This approach — contrary as it is to the Article 29 Working Party’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.’

- ‘There is also a competing interest on the part of users within Europe to access versions of search other than their own.’

- ‘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.’

Further, the Advisory Council noted:

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

---

30 Advisory Council (n 19) 20. One member of the Advisory Council — Sabine Leutheusser-Schnarrenberger — expressed a dissenting opinion on this matter (ibid 26-27): ‘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.’

31 ibid 19-20.

32 ibid 20.

the rights of the data subject adequately in the current state of affairs and technology.\textsuperscript{34}

A central question is then the extent to which delisting will affect these 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.\textsuperscript{35}

The interesting parts 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.\textsuperscript{36} (footnote omitted)

On this point, the Article 29 Working Party’s Guidelines noted that:

it appears that some search engines have developed the practice of systematically informing the users of search engines of the fact that some results to their queries have been de-listed in response to requests of an individual. If such information would only be visible in search results where hyperlinks were actually de-listed, this would strongly undermine the purpose of the ruling. Such a practice can only be acceptable if the information is offered in such a way that users cannot in any case come to the conclusion that a specific individual has asked for the de-listing of results concerning him or her.\textsuperscript{37}

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

\textsuperscript{34} Advisory Council (n 19) 19.
\textsuperscript{35} ibid 21.
\textsuperscript{36} Advisory Council (n 19) 21.
\textsuperscript{37} Art 29 Data Protection Working Party (n 16) 9.
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.\(^{38}\) (footnotes omitted)

The Article 29 Working Party’s Guidelines express a clear view on this point:

Search engine managers should not as a general practice inform the webmasters of the pages affected by de-listing of the fact that some webpages cannot be acceded from the search engine in response to specific queries. Such a communication has no legal basis under EU data protection law.\(^{39}\)

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 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.\(^{40}\) (emphasis added)

\(^{38}\) Advisory Council (n 19) 17.

\(^{39}\) Art 29 Data Protection Working Party (n 16) 10.

\(^{40}\) Advisory Council (n 19) 19.
However, when the reader reaches the fifth and final paragraph relating to the issue of the geographical scope, that message has been dropped. As noted above, it reads as follows:

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.\(^{41}\)

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 will thereby overlook the crucially important caveat included in the second paragraph.

3.3 The Necessity of a Consequence-focused Approach

Advocate General Jääskinen adopted what I elsewhere\(^{42}\) have termed a ‘consequence-focused approach’; that is, rather than restricting himself to a blind adherence to the exact wording of the Directive (a literal interpretation), he sought to identify the consequences of the various possible interpretations; indeed, this approach can be seen as the leading light throughout his reasoning:

In the current setting, the broad definitions of personal data, processing of personal data and controller are likely to cover an unprecedentedly 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.\(^{43}\) (footnote omitted)

\(^{41}\) ibid 20. Recall, though, the dissenting opinion of one of the Advisory Council’s members — Sabine Leutheusser-Schnarrenberger (n 30).


\(^{43}\) Opinion of Advocate General Jääskinen in Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD) (Case C-131/12) at [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 strictly consistent with the text of the Directive — as the *Lindqvist* case taught us, it simply 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.

At any rate, those, like the Article 29 Working Party, who attempt to impose global blocking based on local European values cannot be viewed in isolation. As has been made clear through cases such as 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. Yet 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 oppressive dictatorships seek global removal of content offensive to their laws, supporters of the Article 29 Working Party’s Guidelines can hardly protest based on the effect such removal may have in open tolerant and democratic States. 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. Indeed, no matter what the European

---

44 Case C–101/01 *Criminal Proceedings against Bodil Lindqvist* [2003] ECR I-12971. There, a woman — Bodil Lindqvist — uploaded a website on which she made available personal information about herself and her husband, as well as personal information relating to a number of her colleagues in the church community for which she worked. The website, which was published without the permission of her colleagues, generated some complaints and the matter ended up in court. The legal proceedings related to a range of matters. Interestingly, one of them was whether Lindqvist’s conduct meant she had transferred the data in question to a third country. Instead of adopting a strict literal interpretation, the Court looked to the consequences that would flow from such an interpretation: ‘If Article 25 of Directive 95/46 were interpreted to mean that there is “transfer [of data] to a third country” every time that personal data are loaded onto an internet page, that transfer would necessarily be a transfer to all the third countries where there are the technical means needed to access the internet. The special regime provided for by Chapter IV of the directive would thus necessarily become a regime of general application, as regards operations on the internet. Thus, if the Commission found, pursuant to Article 25(4) of Directive 95/46, that even one third country did not ensure adequate protection, the Member States would be obliged to prevent any personal data being placed on the internet.’ (ibid para 69).

45 See further Svantesson (n 42).

46 ibid.


49 On this the Council noted how ‘[t]he 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 (n 19) 20.
Commission is trying to tell us, this is not a myth. After all, put succinctly, 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. The solution we adopt must fit all legal systems, not just trusted democratic European legal systems.

Given the above, I maintain the position I expressed elsewhere: 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 broad application cannot be excluded based on the wording of the judgment. (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 topic is beyond the scope of this article. 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' — a right to a fair first impression — 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.

Indeed, 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


51 Swantesson (n 33).

52 Kuner (n 12).
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. 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.53

3.4 Seeing the Nuances in a Complex Grey Zone

In many ways, it is surprising that the debate about the geographical scope of the implementation of the Google Spain case has been so heavily focused on top-level domain names (TLDs). After all, such TLDs are merely proxies that generally, but not always, indicate a connection with a particular state. Consider, for example, the TLD .nu formally associated with the small island nation of Niue, but commonly used by Swedish websites as “nu” means “now” in Swedish. It is also surprising that so-called geo-location technologies have not featured more in the discussions.54 Such technologies allow the accurate identification of Internet users’ geographical locations and can (and do) play a significant role in the Internet architecture — even though, up until recently, they have largely been overlooked by European courts and regulators.55 I have discussed these matters in detail in the context of Internet intermediaries being asked to block content and will not repeat that discussion here.56 I merely note that geo-location technologies may both replace and supplement the focus on TLDs.

At any rate, elsewhere57 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 requests, the delisting ought to be local; in others 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 Working Party, Google and the Advisory Council — as astutely noted by Powles, ‘[i]f delisting is determined on a case-by-case basis, surely the remedy can be too’.58

53 See eg Dan JB Svantesson, ‘Between a Rock and a Hard Place – An international law perspective of the difficult position of globally active Internet intermediaries’ (2014) 30 Computer Law & Security Review 348; and Svantesson (n 33).

54 See, however, Van Alsenoy and Koekkoek (n 12) 113-115.


56 See instead Svantesson (n 33).

57 Svantesson (n 27).

58 Julia Powles, ‘Results May Vary: Border disputes on the frontlines of the “right to be forgotten”’, Slate Magazine (25 February 2015) <http://www.slate.com/articles/technology/future_tense/2015/02/>
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.

**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.\(^{59}\)

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.’\(^{60}\) Furthermore, on 16 March 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.\(^{61}\)

---

\(^{59}\) Svantesson (n 33).
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.\textsuperscript{62}

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.\textsuperscript{63}

This is an important point. Private companies operating search engines are unsuitable, and often unwilling, filters for what is ‘good taste’ for the Internet.\textsuperscript{64} Admitting that not all governments can be trusted, perhaps the better approach, in many countries, 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 deserves to be analysed in detail, but such an analysis falls outside the ambitions of this article. I will restrict myself to observing that 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 and thought-provoking 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’:\textsuperscript{65}

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

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?\textsuperscript{66}


\textsuperscript{63} Advisory Council (n 19) 29.


\textsuperscript{65} Van Alsenoy and Koekkoek (n 12).

\textsuperscript{66} ibid 25-26.
These factors are helpful indeed, but like the four principles I had advocated they could perhaps be complemented by a clearer focus on the types of content in question. Here we can usefully reconnect with the helpful 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 nexus to the forum State. In contrast to Van Alsenoy and Koekkoek, I prefer to stay clear of a focus on territory in this context — a highly problematic focal point, not least in the Internet context. For reasons I have outlined elsewhere, I advocate a departure from our traditional focus on the territoriosity principle in favour of what I see as a more contemporary approach, focused on ‘substantial connections’, ‘legitimate interests’ and ‘competing interests’.

Combining all this then, the following Model Code could be advanced:

**Model Code Determining the Geographical Scope of Delisting Under the Right To Delisting**

**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.

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

---

68 Alternatively this Article could be given a somewhat broader wording, such as: ‘[w]here 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.’
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;

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 impact 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,

then 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 Code 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 ‘the local domain’ for example.

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. Indeed, Google’s decision to extend delisting to all EU domains can be viewed as an example of this principle already being applied, be as it may, limited to the EU only. Admittedly, there may 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 for complications in mind, it may be that Article 2 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 — a rule of thumb — 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 expose the data subject to a serious risk of fraud or theft may, of course, be a legitimate 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 are only of concern when they are accessed by a third person with a connection to the data subject. Other types 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 4 focuses on whether there is a substantial connection and a legitimate interest. Indeed, the Article 29 Working Party also 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.69

69 Article 29 Data Protection Working Party (n 16) 8.
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. This Model Code, while intentionally structured as a ‘ready-to-implement’ instrument, should merely be seen as a starting point for further discussions. Several aspects of it surely need to be fleshed out further, and as I have sought to emphasise in the discussion above, not all aspects of it should be seen as ‘set in stone’.

4. Concluding Remarks

It is both amazing and amusing how a well-chosen expression may capture our imagination. ‘Cloud computing’, ‘big data’, ‘the Internet of things’ 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. Is there not something odd and unsettling 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’ — a label not used by the CJEU apart from when referring to what others had argued — has attracted considerable attention for some years now, both in legal circles and in media. 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) was introduced in the mid-1990s. So the thought that the current debate influenced the CJEU’s willingness to embrace a right to be forgotten in Google Spain is difficult to escape. At any rate, not least since the Court avoided adopting the ‘right to be forgotten’ label, it seems to me that no such right 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.

So does the difference between a duty and a right matter here? 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. Secondly, as was referred to more generally above, the labels guide, or even control, our thinking to a large extent.

70 This section partly draws, and expands, upon: Dan JB Svantesson, “‘Right to be Forgotten’ v ‘Duty to be Forgetful’”, and the Importance of Correct Labelling (23 August 2014) <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/> accessed 14 September 2015.
In the text above, I have sought to draw attention to the jurisdictional issues that stem from the *Google Spain* decision. More specifically, I addressed the question of the geographical scope of the right to be forgotten. After all, this matter goes directly to the future implications of the judgment. Just how controversial this issue is can be seen with great clarity in light of the fact that while the Article 29 Working Party’s Guidelines on the implementation of the judgment specifically call for delisting to go beyond the EU domains, recommendations of the Advisory Council to Google on the Right to be Forgotten specifically call for delisting 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 here we should adopt a consequence-focused approach. To that end, I proposed a *Model Code Determining the Geographical Scope of Delisting Under the Right To Delisting*. 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. While the Model was presented in the EU context, it can of course easily be transplanted into other jurisdictions as well.

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. Indeed, it can perhaps be expected that some of the approaches we adopt pursuant to implementation of the *Google Spain* case will colour the implementation of any equivalent right(s) found in the General Data Protection Regulation (in particular Article 17) once it comes into force.