07/14/2014 DRAFT FOR COMMENT

The Right to be Relevant through Obscurity: Why the European Court of Justice Decision is Not Surprising

On May 13, 2014, the Court of Justice of the European Union (Court) issued Press Release No 70/14 announcing its judgment in *Google Spain SL, Google Inc* v *Agencia Espanola de Proteccion de Datos, Mario Consteja Gonzalez.* Many commenters interpreted the Court's opinion as a call for a new "Right to be Forgotten." Legal and internet policy experts reacted to the decision as if the Court had demanded the burning of a library of books containing the collective history of mankind. One legal commentator referred to the members of the court as "clinically insane" and another referred to them as "myopic luddites". I disagree with these assessments based on my analysis of European law and the language of the opinion. My analysis points to four main conclusions:

- **The opinion is a straightforward application of existing European law, substantially limited to the facts of the case. The Court's rulings do not reflect the judges' desire for new legislation or policy.**
- **The opinion does not result in censorship as it explicitly permits the publishing of the information at issue in the case.**
- **The opinion does not cause any information to be "forgotten" as the information at issue can still be found with different search terms.**
- **There is no question that the opinion will present challenges and pose questions for search engines and data brokers that must comply with the court's findings. More guidance is necessary to help companies efficiently and consistently arrive at appropriate decisions about when links to results should be removed.**

The Facts and Procedure of the Case - In January and March of 1998, the La Vanguardia newspaper published information about a real estate auction held to recover Mr. Costeja Gonzalez's social security debts. In 2010, Mr. Costeja Gonzalez entered a complaint with the Agencia Espanola de Proteccion de Datos (the Spanish Data Protection Agency, known as the AEPD), stating that upon entering his name, the Google search engine would display links to pages of the 1998 La Vanguardia newspaper entries posted on the internet. Mr. Costeja Gonzalez asked that La Vanguardia remove the references to his name from the internet postings of the original newspaper pages, and that Google and its Spanish subsidiary should remove links to those pages from the results of searches of his name. The AEPD rejected the demand that La Vanguardia delete the references in the online newspaper, but upheld the request that Google adjust the search results so they would not return links to those pages in response to a query of Mr. Costeja Gonzalez's name. Google appealed to the Audiencia Nacional (the National High Court of Spain), which in turn referred three questions about European law to the Court. The Court's response to those questions prompted a global discussion about "The Right to be Forgotten".

The Three Questions (I am greatly simplifying the questions here, as they have many subparts in the filings)**:**

1. **Jurisdiction –** Should the provisions of the Directive (under which the Spanish data protection law is implemented) apply to Google with respect to the Google search engine's response to a

query to its search engine, when that query is the name of an individual living in Spain, and the results provide links to the website of a Spanish newspaper?

2. **Controller/Processing –** If the provisions of the Directive apply to this type of search, should Google and/or its Spanish subsidiary be held to be Controllers (as defined by the Directive) who are Processing (as defined by the Directive) personal data?
3. **Forgetting –** Should an individual have the ability to lodge a complaint to prevent a search engine from linking to information lawfully published by third parties?

Rulings:

In response to the three questions above, the Court issued a 23 page opinion, which includes four main concluding rulings:

1. **Jurisdiction**: When a search engine sets up an activity to sell online advertising that will relate to the search engine query results, then such activities are subject to the jurisdiction of the European Union Member State where those online advertising activities are located.
2. **Controller/Processing:** The activities of a search engine (finding, indexing, storing, and making available information in a particular order of preference) is the processing of personal data under the Directive, and the operator of the search engine is the Controller.
3. **Removal:** The Directive can require search engines to remove links from a list of results from a query of an individual's name, even if the material to which the information at those links was published lawfully.
4. **Balancing Test:** The individual's rights to request the removal of a list of results based on the search of that individual's name is limited by the economic interest of the search engine operator, and the interest of the general public, and the interference with the individual's rights can be justified by the "preponderant interest of the general public".

None of these four conclusions are surprising, if we look at the Directive and existing European Law. Let's take each one in turn.

Analysis:

I. Jurisdiction: ***The decision relies heavily on the European Union's Article 29 Working Party 2008 analysis of jurisdiction found in its Opinion 1/2008 (WP 148) which in effect states that an entity is subject to the laws of jurisdictions of which it purposefully avails itself.***

The European Union's Article 29 Working Party (the advisory group formed with representatives from each of the EU Member States) previously analyzed the issue of whether the Directive should apply to search engines (WP 148, April 4, 2008) that are not located in an EU Member State. EU data protection law applies in two situations:

1. Where the search engine has an "establishment" in the EU Member State (Article 4(1)(a) of the Directive), or

2. Where the search engine makes use of equipment in the EU Member State (Article 4(1)(c) of the Directive).

WP 148 is an interesting document with respect to the Google case, especially as it focuses on the protection of the personal data of the individual entering the search query, rather than on protection of

the individual who is the subject of the query. It clearly states that an entity does have an "establishment" when it creates "an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state", as long as those advertisements "play a relevant role in the particular processing operation". However, it also says that the use of equipment will not qualify as an "establishment" if used "only for purposes of transit through the territory". (Pages 10 and 11 of WP 148)

The Court determined that Google Spain was in the business of selling advertising linked to the display of results from the query of Mr. Costeja Gonzalez's name. Therefore, it never took up the issue of whether Google's use of automated indexing software on the internet would constitute the "use of equipment" to satisfy the establishment requirement. The Court's adoption of the Working Party's analysis is not surprising: it comports with a considerable body of international law that states that an entity is subject to the laws of jurisdictions of which it purposefully avails itself. The Court concluded that when Google set up an entity in Spain to sell advertising to relate to search query results it became subject to the Spanish data protection law. In other words, if you target an activity to make money in a particular country, you need to be prepared to be subject to its laws.

II. Controller/Processer*: The Court found that Google is a data controller because it determines the purpose and means of organizing personal data. It further found that Google is a data processor based on its analysis that Google's search engine does not simply transmit information but processes and organizes information to help individuals find answers to questions.*

If Google's sale of advertising in Spain subjects it to Spanish data protection law, it is necessary to consider the Court's analysis of whether Google was a "Controller" that was "Processing" personal data according to the Directive.

Article 2(d) of the Directive defines a Controller as "the natural or legal person, public authority, agency or any other body which alone or jointly with others **determines the purposes and means** of the processing of personal data …" (emphasis added). With respect to the indexing of the personal data included in the results of search queries, the Court concluded without much analysis that Google "determines the purposes and means" by the nature of its algorithm organizing the personal data to determine which search results to display, and in what order to display them.

The Court spent more time analyzing whether by providing those search engine results, Google was "Processing" under the law. Article 2(b) of the Directive defines Processing as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." The interpretation of this definition is particularly important. If information intermediaries are found to be "processing personal data" merely by transmitting information through their equipment or software, then application of the law could create a substantial barrier and cost for the operation of the internet. The primary question is whether Google's search engine functions more like a telephone service provider that simply allows the information to pass through, or more like a private investigator that helps individuals find the answers to their questions.

The Court's analysis of this issue is open to debate. In paragraph 28 of the opinion the Court appears to comment on Google's indexing activities when it states "in exploring the internet automatically, constantly and systemically in search of the information which is published there, the operator of a search engine "collects" such data which it subsequently "retrieves", "records" and "organizes" within the framework of its indexing programmes, "stores" on its servers and, as the case may be "discloses" and "makes available" to its users in the form of lists of search results. In paragraph 41 the Court appears to rely upon the fact that Google displays results "according to a particular order of preference" and therefore must be deemed to be "processing personal data". The Court's conclusion is also supported by the Working Party opinion on search engines which states, "Search engines process information, including personal information, by crawling, analyzing and indexing the World Wide Web and other sources they make searchable and thereby easily accessible through their services." (Page 13 of WP 148).

Google's success in the marketplace has depended on its ability to accurately determine what results individuals want to see. The Court appears to be saying that indexing based on the importance to the searcher makes the company's search engine activities function more like the private investigator and less like the telephone service provider. The Court's conclusion may be difficult to align with the body of law in Europe and the United States that determines whether an information intermediary can be liable for the content delivered over its website and network. Article 12 of the European Union's E-Commerce Directive addresses this issue by asking whether the internet service is acting as a "mere conduit" of the information. Under this definition the European Union exempts the company from liability if it satisfies the following three conditions:

(a) does not initiate the transmission;

(b) does not select the receiver of the transmission; and

(c) does not select or modify the information contained in the transmission.

The Court appears to be of the opinion that Google's use of an algorithm to index information and determine what results to provide to the search query causes it to fail part (c) of this test, as it "selects" the information in the results. Other countries have different standards for determining information intermediary liability (such as Section 230 of the Communications Decency Act in the United States), and may come to a different result.

III. Removal: *The Court was not charged with making a global public policy recommendation, but instead to answer specific questions of European law. The Court applied the law narrowly, addressing only the question of what constitutes a relevant and proportionate response to a search query of Mr. Costeja Gonzalez's name.*

If we now see the reasons why the Court determined Google was subject to Spanish Data Protection Law, and that they satisfy the definitions of Controller and Processing in this context, we next need to analyze how the Court interpreted the Directive to apply to Google.

The Court spends little time considering what it means to be "forgotten" or "consigned to oblivion". In fact, the Court's four rulings do not include the words "forgotten", "forgetting" or "oblivion". The Court's analysis only includes these words to refer back to the Spanish court's questions (paragraph 89) or to reference arguments made by the parties to the case (paragraphs 90 and 91). Rather, the Court

spends the majority of its opinion describing how Mr. Costeja Gonzalez's request for deletion of the links fits squarely within Article 6 (1)(c) of the Directive. (paragraphs 72 and 92)

The Directive's Article 6 (1) (c) requires "that personal data must be … adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." The Court analyzes this provision of the Directive by asking what the "further processing" of the information was in this context. (paragraph 98). On this point, the Court applies the law quite narrowly, and states several times that it is only asking the question of what results are a relevant and proportionate response to a search query of Mr. Costeja Gonzalez's name. The Court does not determine whether those same results would have been appropriate for searches of "Costeja Gonzalez real estate auction", "La Vanguardia social security debts" or "1998 real estate auctions". Given the repeated language in the opinion limiting application of the rule only to results responding to queries of Mr. Gonzalez's name, it is reasonable to think the Court may have decided the linked pages at issue in the case would have been appropriate for searches specifically targeting Mr. Gonzalez's real estate affairs and social security debts.

So, why has such a limited ruling created such a stir about "The Right to be Forgotten"? Apparently some of the language in the background portion of the opinion, and the way it intersects with the European Union's current attempts to revise the Directive, created the mistaken impression that the Court was creating such a right.

Popular media incorrectly report that the Court's opinion establishes a "Right to be Forgotten." While that term describes a portion of the proposed General Data Protection Regulation (Regulation) currently under consideration and that would replace the Directive, some of this confusion was created by the way in which the question was posed in the case. The Spanish Court asked the Court the following:

> 3. Regarding the scope of the right of erasure and/or the right to object, in relation to *the "derecho al olvido" (the "right to be forgotten"),* (emphasis added) the following question is asked:
>
> > 3.1 must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by Article 14(a), of Directive 95/46/EC, extend to enabling the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be *consigned to oblivion*, (emphasis added) even though the information in question has been lawfully published by third parties?

Question 3 is a fairly straightforward request for analysis of the provisions of the Directive. However, both the language in the header (emphasized), stating that the question should be evaluated in the context of derecho al olvido ("the right to be forgotten) and its inclusion of a phrase about the

individual asking that the information be "consigned to oblivion" (also emphasized) create an impression that the court's holding is broader than it is in fact.

Many legal commentators and companies have expressed concern with the European Union's attempts to place a "Right to be Forgotten" in the Regulation. The European Commission's initial establishing this right included broad obligations requiring online publishers to go back to the sources or where references to personal data were originally posted or processed and delete the information. If possible, this might have created some type of "forgetting" or "oblivion", but the language was widely criticized as being impossible to implement. More recent language from the European Parliament has substantially narrowed the obligation to be very close to the current provisions in Article 6(1)(c) of the Directive. The header "The Right to be Forgotten" remains in the draft Regulation's text, but the provision now would be more accurately titled "The Right to Relevance", and is in line with the Court's rulings.

IV.Balancing Test: ***The Court relied on the legal obligation set forth in the Directive that data be "adequate, relevant and not excessive" in determining that the processing purpose of indexing information based only on a query of an individual's name did not outweigh the impact on the individual's privacy.***

As noted above, the Directive provides a legal obligation that the data be "adequate, relevant and not excessive". The Court's opinion, contrary to its depiction in the media, creates a narrow, fact-based determination that 16 year old real estate debts are not relevant enough in this context. The Court determined that in this instance the purpose of indexing information just based on a search query of an individual's name did not outweigh the potential impact on the individual's right to privacy. However, neither the Spanish court, nor the Court of Justice, required that the underlying newspaper articles should be deleted from the internet. Interestingly, the Court in a sense said that Google's algorithm did a poor job in indexing the search results. Google attempts to provide search results that are as relevant as possible for the searcher. Many believe it is this organizing based on the relevance of the results that provides Google a competitive advantage compared to other search engines. The Court's opinion also raises the additional question that even if some search results are deemed "relevant", when would they be deemed "excessive"? What does "excessive" mean in the context of a search engine? These are important questions, but the facts of this case did not require the Court to fully examine them. Instead, the Court appears to rely upon the facts of the case that the newspaper articles were 16 years old and were not currently relevant for a search of Mr. Costeja Gonzalez's name.

In a discussion many years ago about privacy legislation a colleague used the hypothetical of an internet company call www.spyonyourneighbor.com. He asked whether privacy legislation should prohibit the use of personal data to spy on individuals. After some discussion, we determined "spyonyourneighbor.com" was not a hypothetical business, but rather an aspect of the way search engines can function. The Court addressed that capability of search engines straight on, and determined that displaying results to a search engine query of an individual's name requires that those results comply with Article 6 of the Directive. While this ruling now creates complexity and highlights important policy considerations related to the free flow of information, it does not result in complete "forgetting", as more precise searches could still provide results that link to the information.

Moreover, the result is not surprising, as it is a straightforward interpretation of the relevancy requirements of Article 6. The result is, therefore, much more about obscurity (as Profs. Woodrow Hartzog and Evan Selinger have written) than it is the Right to be Forgotten. I have also written about the value of using obscurity to protect privacy. And for those who incorrectly assume these concepts of relevance and obscurity are only European or theoretical, Marty Abrams has described both how important the concepts are and how they form the basis for some of the U.S.'s most effective current privacy legislation (the Fair Credit Reporting Act).

Where Do We Go From Here

The Spanish court now must issue its own ruling under the Spanish implementing legislation in accordance with the Court's opinion. Similarly, other EU Member State data protection authorities will need to interpret the opinion as they apply their laws. This lack of harmonization in the member state implementing legislation and member state interpretation of the Directive continues to be a serious compliance problem for multi-national companies. We now know the Court thinks 16 years is too old for data to be relevant in this context. What about 12 years, or 10, or 5? It is difficult to predict how 28 different member states will interpret the need to balance between the rights of the individual and the "preponderant interest of the general public." While arriving at that harmonization was not, of course, the Court's job in answering the questions posed in the case, its decision creates a pressing need now for further guidance. It also points to one of the main problems with the current European system of a Directive that creates a floor, but not a ceiling, for member states. The case provides an example of why it is important to further pursue concepts like the "one-stop-shop", which the European Commission proposed in the Draft General Data Protection Regulation as a means to provide more predictability and harmonization across Europe.

Also, while this opinion is limited to one particular query on search engines, the concepts it explores also apply to much of U.S. Federal Trade Commission's (FTC) analysis of the data broker industry. The FTC specifically called out the challenges to privacy that come from data brokers that provide "people search" services. The FTC unanimously recommended in their report:

> "that Congress consider legislation requiring data brokers offering people search products to: (1) allow consumers to access their own information; (2) allow consumers to opt out of the use of the information; (3) clearly disclose to consumers the data brokers' sources of information, so that, if possible, the consumer can correct his or her information at the source; and (4) clearly disclose any limitations of the opt out, such as close matches of the individual's name may continue to appear in search results." (FTC Report, P. 54)

The FTC report shows that regulators on both sides of the Atlantic are concerned about the privacy implications of services that allow easy access to large amounts of an individual's personal information based solely on a search of that individual's names. The FTC report also points out that this concern is not new, but was a motivation for the Fair Credit Reporting Act in the 1970's, and is the reason the Individual Reference Services Group temporarily established a self-regulatory program to provide more transparency into such services. (FTC Report, P. vii).

The Courts opinion creates substantial implementation problems for search engines and data brokers that must determine when links to information should be removed. Companies in these businesses may err on the side of caution to avoid regulatory action, and comply with requests to remove links to

content in more situations than just search results from the query of an individual's name. By doing so, these compliance efforts may result in greater limits on the free flow of information than are necessary to protect individual privacy.

One way to deal with the complexity of implementing the Court's guidance would be to establish a centralized body which would handle "obscurity requests" from individuals. Regulators could provide search engines and data brokers with liability protection from following the direction of such a centralized obscurity center. The obscurity center could function as a co-regulatory body with companies voluntarily participating, but agreeing to regulatory oversight of both the organization and whether participating companies follow through with the obscurity center's recommendations. The result would be a more efficient system, which removes the burden of making these determinations from each individual company, while providing individuals with reasonable access to a remedy.

Conclusion

In light of the provisions of the Directive, the Court was neither insane, nor near sighted. The Court's opinion has furthered a discussion that requires more analysis and creative thinking about how to create individual trust in the use of our digital infrastructure. Finding methods to implement the Court's opinion will be difficult, and must guard against the unintended consequence of harming free expression. However, continued discussion of the limited nature of the Court's rulings, and exploration of ways to analyze what information should be obscured are both possible and necessary. That exploration is critically important at a time where we see efforts to put in place new privacy laws around the world, among them the EU Draft General Data Protection Regulation.