UNC SCHOOL OF LAW

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY

Volume 17 | Issue 3 Article 2

3-1-2016

The Right to Obscurity: How We Can Implement the Google Spain Decision

David Hoffman

Paula Bruening

Sophia Carter

NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 17, ISSUE 3: MARCH 2016

THE RIGHT TO OBSCURITY: HOW WE CAN IMPLEMENT THE *GOOGLE SPAIN* DECISION

David Hoffman*
Paula Bruening**
Sophia Carter****

On May 13, 2014, the Court of Justice of the European Union ("CJEU") announced its judgment in Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Consteja González*. The decision required Google to delist certain internet search results when a search query was made using an individual's name. Commentators worldwide have referred to this delisting as the Right to be Forgotten. This article analyzes the legal background of the case, and the implications for technology companies and individuals. Specifically, the article concludes the required delisting is much more about obscurity than forgetting. The article concludes by making a recommendation for how to create an obscurity center, which could implement the delisting requests.*

* David Hoffman is Associate General Counsel and Global Privacy Officer at Intel Corporation. He is a graduate of Hamilton College and the Duke University School of Law, at which he holds a Senior Lecturing Fellow academic appointment.

** Paula Bruening is Senior Counsel, Global Privacy Policy at Intel Corporation. She is a graduate of John Carroll University and the Case Western Reserve University School of Law.

*** Sophia Carter is a graduate of George Washington University and the Duke University School of Law.

I. INTRODUCTION

On May 13, 2014, the Court of Justice of the European Union ("CJEU") announced its judgment in *Google Spain SL, Google Inc.* v. *Agencia Espanola de Proteccion de Datos, Mario Consteja González* ("*Google Spain*").[1] The decision handed down by the CJEU,[2] has generated considerable controversy in the European Union ("EU") and internationally.[3]

The increasingly connected and personal nature of technology highlights the importance of this case. Individuals not only carry personal technology, such as smart phones,[4] but many devices in the home connect directly to the internet, including cameras, microphones, and motion sensors. These devices give service providers an increasingly accurate and detailed view of an individual's activities and location and a more comprehensive picture of what happens in the home. Any of this information could be posted to the Internet (1) if a service provider buries the right to do so in lengthy terms and conditions, (2) as a result of a data breach, or (3) by an unscrupulous employee of the service

---

[1] Press Release No 70/14, Court of Justice of European Union, Judgment in Case C-131/12 Google Spain, SL, Google Inc. v. Agencia Espanola de Proteccion de Datos, Mario Costeja Gonzalez (May 13, 2014), http://curia.europa.eu.

[2] Because the CJEU is located in Luxembourg, it is often referred to in academic papers as the Luxembourg CJEU, not to be confused with the European CJEU of Human Rights (ECHR), which is located in Strasbourg, France.

[3] *See, e.g.*, Amber Melville-Brown & Caroline Thompson, *Who-ogle? Rehabilitation in the Digital Age*, THE TIMES (Oct. 23, 2014), http://www.thetimes.co.uk/tto/law/article4244517.ece; Robert Peston, *Why Has Google Cast Me Into Oblivion*, BBC NEWS (Jul. 2, 2014), http://www.bbc.com/news/business-28130581. Jeffrey Rosen called the concept a major threat to free expression, even before *Google Spain*. *See* Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88, 90–92 (2012), http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

[4] Today, 68% of U.S. adults have a smartphone, up from 35% in 2011, and tablet computer ownership has edged up to 45% among adults. Smartphone ownership is nearing saturation with some groups: 86% between the ages of 18 and 29 have a smartphone, as do 83% of those between the ages of 30 and 49, and 87% of those living in households earning $75,000 and up annually. Monica Anderson, *Technology Device Ownership: 2015*, PEW RESEARCH CENTER (2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

provider. How the CJEU opinion is interpreted and implemented in the time directly following the CJEU decision will have a lasting impact on the ability of individuals to rectify situations where this data is posted to the Internet.

Many commentators interpreted the CJEU's opinion as a call for a new "Right to Be Forgotten."[5] Legal and policy experts who study Internet privacy reacted to the decision as if the CJEU had demanded the burning of a library of books containing the collective history of mankind. One legal commentator referred to the CJEU judges as "clinically insane;"[6] another referred to them as "European luddites."[7] This paper analyzes the decision and disagrees with this assessment based on the authors' understanding of European law and the language of the opinion.

This paper first provides an overview of the case and the legal foundations of the decision. It analyzes the ruling in the context of the 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Directive").[8] Finally, this paper explains why the authors disagree with many criticisms of the ruling.

Based on our analysis, we reach the following conclusions:

(1) The opinion is a straightforward application of existing European law, substantially limited to the facts of the case. The CJEU's rulings do not reflect a desire on the part of the judges for new legislation or policy.

---

[5] *See, e.g.*, Jonathan Zittrain, *Don't Force Google to Forget*, N.Y. TIMES (May 14, 2014), http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html.

[6] *Steptoe Cyberlaw Podcast – Interview with David Hoffman,* STEPTOE CYBERBLOG (Sept. 3, 2014), at 00:34:39, http://www.steptoe.com/staticfiles/SteptoeCyberlawPodcast-032.mp3.

[7] Michael Wolff, *Wolff: The Right to be Forgotten by Google*, USA TODAY (May 18, 2014), http://www.usatoday.com/story/money/columnist/wolff/2014/05/18/a-big-setback-for-google-in-europe/9172941/.

[8] Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31 [hereinafter Data Protection Directive].

(2) The opinion's impact on free expression is substantially mitigated as it explicitly permits the publishing of the information at issue in the case. Moreover, providing the opportunity for limited obscurity actually encourages free expression.

(3) The opinion does not result in the actual "forgetting of any information," as the information at issue can still be found using different search terms.

(4) The opinion will present challenges and pose questions for search engines and data brokers that must comply with the CJEU's findings. More guidance is necessary to help companies efficiently and consistently arrive at appropriate decisions regarding delisting certain answers from Internet searches.

Key to our analysis of the case is the idea that the legal rights involved are not about "forgetting" but instead involve "obscurity." This paper distinguishes these terms and demonstrates that the legal basis for the ruling in *Google Spain* is the Directive's language providing for the limited ability for erasure.[9] In the case of *Google Spain*, application of this provision would involve not deleting or removing the newspaper article in question, but rather making it necessary to enter more refined search terms than simply a person's name to discover the article. This limited erasure right is quite different from concepts of "forgetting," which would require going back to source documents on the internet and making certain that references to the primary material were removed entirely or rendered not obtainable. Thus, rather than "forgetting," the application of the Directive's erasure provisions to search engine results provides for "the right to obscurity."

The paper, then analyzes the case in light of developments in the law since 2014, looking to case law from the European Court of Human Rights ("ECHR") to provide context for the CJEU decision.[10] Finally, the paper focuses on future developments and approaches to the issue within Europe and in other jurisdictions.[11]

---

[9] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶ 100 (June 25, 2013).

[10] *See infra* Part IV.E.

[11] *See infra* Part V.

Although the ruling is a predictable interpretation of the language of the Directive, practical questions and concerns remain. The CJEU decision unfairly burdens Google and other search engine companies with determining when a request for obscurity should be granted. The paper proposes that this burden could be removed and calls for implementation of a global solution the authors refer to as the "Internet Obscurity Center."[12]

II. FACTS & PROCEDURE OF *GOOGLE SPAIN*

In January 1998 and March 1998, the *La Vanguardia* newspaper published information about a real estate auction held to recover Mr. Costeja González's social security debts.[13] In 2010, Mr. Costeja González, a Spanish citizen, filed a complaint with the *Agencia Espanola de Proteccion de Datos* ("AEPD")[14] against *La Vanguardia*. He alleged that when an Internet user entered his name in Google's search engine the user would be provided with links to the 1998 *La Vanguardia* newspaper entries announcing a foreclosure auction on Mr. Gonzalez's home.[15] Mr. Costeja González asked that *La Vanguardia* be required to remove the references to his name from the Internet postings of the original newspaper pages, and that Google and its Spanish subsidiary remove links to those pages from the results of searches of his name.[16] The AEPD rejected the demand that *La Vanguardia* delete the references in the pages of *La Vanguardia* newspaper posted online, but granted the request that Google adjust the search results

---

[12] *See infra* Part VI.

[13] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, at ¶ 14 (May 13, 2014).

[14] The AEPD is the Spanish data protection authority. It is the national independent public authority responsible for ensuring compliance with data protection law. The Data Protection Agency interprets, applies and disseminates data protection law, maintains the General Data Protection Registry, safeguards citizens' data protection rights, and authorizes international data transfers. *Data Protection in Spain: Overview,* PRACTICAL LAW (Dec. 1, 2015), http://uk.practicallaw.com/1-520-8264#a246427; *see* Agencia Española de Protección de Datos, www.agpd.es (last visited Feb. 18, 2016).

[15] *Google Spain*, 2014 E.C.R. 317, at ¶ 14.

[16] *Id.* at ¶ 15.

so they would not return links to those pages in response to a query of Mr. Costeja González's name.[17] Google appealed to the *Audience Nacional*, which in turn referred three questions about European law to the CJEU.[18] The three questions relate to jurisdiction, the role of the data processor, and data removal.[19] The CJEU's response to these questions prompted a global discussion about a so-called "Right to be Forgotten."[20]

III. THE LEGAL FOUNDATIONS OF *GOOGLE SPAIN*

The CJEU decided *Google Spain* based on the Directive and the relevant provisions of the Charter of Fundamental Rights.[21] Analysis of the decision requires an understanding of these two documents.

Data protection in the European Union is primarily governed by the Directive.[22] The Directive was enacted based on Article 114(1) of the Treaty on the Functioning of the European Union ("TFEU").[23] Article 114(1) states generally that the European

---

[17] *Id.* at ¶¶ 16–17.

[18] *Id.* at ¶¶ 17–20.

[19] *See infra* Part IV.

[20] *See, e.g.*, *Debate: Should The U.S. Adopt The 'Right To Be Forgotten' Online?*, NPR (Mar. 18, 2015), http://www.npr.org/2015/03/18/393643901/debate-should-the-u-s-adopt-the-right-to-be-forgotten-online; Julia Powles & Enrique Chaparro, *How Google Determined Our Right to be Forgotten*, THE GUARDIAN (Feb. 18 2015), http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search.

[21] The European Charter of Fundamental Rights contains rights and freedoms under six titles: Dignity, Freedoms, Equality, Solidarity, Citizens' Rights, and Justice. The charter became legally binding in 2009 with the treaty of Lisbon. *See EU Charter of Fundamental Rights*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/fundamental-rights/charter/index_en.htm [hereinafter European Charter].

[22] EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *Handbook on European Data Protection Law* 17 (2014), http://fra.europa.eu/sites/default/files/fra-2014-handbook-data-protection-law-2nd-ed_en.pdf.

[23] ORLA LYNSKEY, *From Market-Making Tool to Fundamental Right: The Role of the CJEU of Justice in Data Protection's Identity Crisis*, in EUROPEAN DATA PROTECTION: COMING OF AGE 59, 60 (Serge Gutwirth et. al. eds., 2013); *see also* Consolidated Version of the Treaty on the Functioning of the European Union art. 114, May 9, 2008, 2008 O.J. (C 115) 47 [hereinafter TFEU] (explaining the authority for the adoption of the Directive).

Council and the Parliament may enact laws and measures to ensure the proper functioning of the internal market.[24]

As required by law, the CJEU interpreted the facts of the case and the Directive in light of the applicable provisions in the Charter of Fundamental Rights ("European Charter").[25] The Charter, adopted in 2000, has been "a legally binding instrument of EU law since late 2009, binding both the EU institutions and the Member States . . . ."[26] The Charter is referenced in Article 6 of the Lisbon Treaty.[27] The Lisbon Treaty modified two pre-existing treaties governing the mechanisms for operating the European Union.[28] When it came into force on December 1, 2009, it established the Charter as legally binding. The extent to which provisions of the Charter can be directly enforced by Member States of the CJEU is not clear. However, Articles 7 and 8 of the Charter—which articulate the rights to Respect of Privacy and Family Life and Protection of Personal Data—are foundational to understanding privacy and data protection rights in the European Union.[29] The key provision in the Charter applied by the CJEU in *Google Spain* is Article 8, which makes clear that data that relates to an individual must be processed fairly.[30]

---

[24] TFEU, *supra* note 23.

[25] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, ¶ 1 (May 13, 2014) ("This request for a preliminary ruling concerns . . . Article 8 of the Charter of Fundamental Rights of the European Union."); *see also* European Charter, *supra* note 21.

[26] Gráinne de Búrca, *After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?*, 20 MAASTRICHT J. OF EUR. & COMP. L. 168, 169 (2013).

[27] Art. 6(1) of the Treaty on the European Union ("TEU"), as amended by the Treaty of Lisbon, states that the Union recognizes "the rights, freedoms and principles set out in the Charter . . . which shall have the same legal value as the Treaties." *See* Consolidated version of the Treaty on European Union art. 6(1), Oct. 26, 2012, 2012 O.J. (C 326) 13, 19.

[28] *Id.*

[29] PAUL DE HERT & SERGE GUTWIRTH, *Data Protection in the Case Law of Strasbourg and Luxembourg: Constitutionalism in Action*, 18 REINVENTING DATA PROTECTION? 3, 7 (Serge Gutwirth et. al. eds., 2009).

[30] European Charter, *supra* note 21, at 10. The relevant articles state:
Article 7 Respect for private and family life

It is also important to understand the distinction between the Charter and the European Convention on Human Rights ("the Convention").[31] The Convention was adopted in 1953 by the Council of Europe.[32] While all of the members of the European Union are also members of the Council of Europe, the two institutions and their roles are separate and distinct.[33] The Council of Europe created the European Court of Human Rights ("ECHR") to interpret the Convention.[34] When the EU began its process to create the Charter, the provisions of the Convention served as its starting point.[35] The language of the two documents is similar and their provisions overlap in some areas.[36] As a consequence,

---

> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8 Protection of personal data
>
> 1. Everyone has the right to the protection of personal data concerning him or her;
>
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified;
>
> 3. Compliance with these rules shall be subject to control by an independent authority.

Id.

[31] Convention for the Protection of Human Rights and Fundamental Freedoms, Nov. 4, 1950, 213 U.N.T.S. 222 [hereinafter European Convention].

[32] *See* Aisa Gani, *What is the European Convention on Human Rights?*, THE GUARDIAN (Oct. 3, 2014), http://www.theguardian.com/law/2014/oct/03/what-is-european-convention-on-human-rights-echr (describing the history of the convention and the main principles).

[33] *See* European Convention, *supra* note 31.

[34] *See* EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, *supra* note 22 at 14.

[35] *Compare* European Convention, *supra* note 31 ("Considering that this Declaration aims at securing the universal and effective recognition and observance of the Rights therein declared"), *with* European Charter, *supra* note 21 ("[I]t is necessary to strengthen the protection of fundamental rights in the light of changes in society, social progress and scientific and technological developments by making those rights more visible in a Charter.").

[36] *See, e.g.*, European Charter, *supra* note 21 at art. 52(3) ("[S]o far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning

procedurally "judges first consider the Charter and then adopt other human rights sources . . . ."[37] The jurisprudence of the ECHR is used as a tool of interpretation for CJEU decisions:

> [t]he Court may adopt, with respect to provisions of the Convention, an interpretation which does not coincide exactly with that given by the Strasbourg authorities, in particular the European Court of Human Rights. It is not bound, in so far as it does not have systematically to take into account, as regards fundamental rights under Community law, the interpretation of the Convention given by the Strasbourg authorities.[38]

Article 52 of the Charter prohibits the CJEU from interpreting the law in a way that would contravene the protection of the human rights of a European citizen.[39] In this way, the architects of European law have assured that even if the CJEU does not follow the exact analysis as the ECHR on a similar issue, it must still look to the ECHR case law for guidance. Two prominent Advocates General add that:

> [t]he Convention can be used as a second fundamental source in identifying shared legal positions and the scope of their application. Since its ratification, the [CJEU] increasingly refers to the Convention to determine the basis and scope of fundamental rights. Furthermore, the [CJEU] has explicitly recognized that EU [CJEUs] have to take the case-law of the European Court of Human Rights in Strasbourg into account in interpreting fundamental rights.[40]

---

and scope of those rights shall be the same as those laid down by the said Convention.").

[37] Sonia Morano-Foadi & Stelios Andreadakis, *Reflections on the Architechture of the EU After the Treaty of Lisbon: The European Judicial Approach to Fundamental Rights*, 17 EUR. L. J. 595, 600 (2011), http://www.cesruc.org/uploads/soft/130303/1-130303200129.pdf.

[38] RICK A. LAWSON, *Confusion and Conflict? Diverging Interpretations of the European Convention on Human Rights in Strasbourg and Luxembourg*, THE DYNAMICS OF THE PROTECTION OF HUMAN RIGHTS IN EUROPE - ESSAYS IN HONOUR OF PROFESSOR HENRY G. SCHERMERS 219, 228 (R.A. Lawson & M. de Blois, eds., Martinus Nijhoff Publishers vol. III 1994) (footnote omitted).

[39] Article 52(3) of the European Charter states in part, "[i]n so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention[.]" *See* European Charter, *supra* note 21, at art. 52(3).

[40] Julianne Kokott & Christoph Sobotta, *The Charter of Fundamental Rights of the European Union After Lisbon* 2 (European Univ. Inst. Acad. of European

The CJEU was not charged with making a global public policy recommendation but instead with answering specific questions of European law.[41] The CJEU applied the law narrowly, addressing only the question of what constitutes a relevant and proportionate response to a search query of Mr. Costeja González's name.[42] While the CJEU might appropriately be criticized for failing to take into consideration the policy impact of its decisions, the CJEU is only officially charged with answering the questions of European law posed to it by member state courts.

IV. ANALYSIS: THE MAIN QUESTIONS

Google Spain addresses three questions. The first question relates to jurisdiction: should the erasure rights provision 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, when that query is the name of an individual living in Spain, and the results provide links to the website of a Spanish newspaper?[43] The second question examines the role of the *data processor* and *data controller*:[44] if the provisions of the Directive apply to this type of search, should Google and/or its Spanish subsidiary be considered "controllers" (as defined by the Directive) who are processing (as defined by the

---

Law, EUI Working Paper No. AEL 2010/6, 2010), http://cadmus.eui.eu/bitstream/handle/1814/15208/AEL_WP_2010_06.pdf?sequence=3.

[41] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶ 20 (June 25, 2013).

[42] *Id.* at ¶ 98.

[43] *Id.* at ¶ 20.

[44] Article 2(e) defines a data processor as, "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller." Data Protection Directive, *supra* note 8, at art. 2(e). Article 2(d) defines a data 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; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law.

Id. at art. 2(d).

Directive) personal data?[45] The third question evaluates the notion of removal: should an individual have the ability to lodge a complaint to prevent a search engine from linking to information lawfully published by third parties?[46] Each of these questions are now examined in turn to analyze the reasoning of the CJEU.

A. *Jurisdiction*

The *Google Spain* decision relies heavily on the European Union's Article 29 Working Party 2008 analysis of jurisdiction found in its Opinion 1/2008 ("WP 148").[47] That opinion, in effect, states that an entity is subject to the laws of jurisdictions to which it purposefully avails itself.[48]

The European Union's Article 29 Working Party previously analyzed the issue of whether the Directive should apply to search engines that are not located in an EU member state.[49] According to the analysis, EU data protection law applies in two specific situations: (1) when the search engine has an "establishment" in

---

[45] The Directive defines the "processing" of data 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." *Id.* at ch. 1, art. 1(b).

[46] The Directive defines "third parties" as "any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data." *Id.* at ch. 1, art. 1(f).

[47] *Article 29 Data Protection Working Party: Opinion 1/2008 on Data Protection Issues Related to Search Engines* 00737/EN/WP 148, (Apr. 4, 2008) [hereinafter WP29 Opinion], http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf.

[48] *See, e.g.*, Data Protection Directive, *supra* note 8, at art. 29 (Article 29 of the Directive calls for the establishment of a "working party" of national data protection authorities.); *see also id.* at art. 30. The working group advises the European Commission on the latest challenges in European data privacy, makes recommendations on new legislation and assesses the level of "adequacy" of protection in third-countries. *See generally* Burkard Eberlein & Abraham L. Newman, *Escaping the International Governance Dilemma? Incorporated Transgovernmental Networks in the European Union*, 21 GOVERNANCE 25, 38–39 (2008).

[49] WP29 Opinion, *supra* note 47, at 8–11.

the EU Member state;[50] and (2) when the search engine makes use of equipment in the EU Member state.[51] The analysis is of particular interest in the case of *Google Spain*, because 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.[52] 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."[53] 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."[54]

The CJEU ultimately determined that Google's Spanish subsidiary was in the business of selling advertising linked to the display of search results of the query of Mr. Costeja González's name.[55] 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" sufficient to satisfy the establishment requirement.

The CJEU's adoption of the Working Party's analysis is not surprising: it comports with generally accepted United States law about international jurisdiction that subjects an entity to the laws of jurisdictions of which it purposefully avails itself.[56] The CJEU concluded that when Google set up an entity in Spain to sell advertising related to search query results, it became subject to the Spanish data protection law.[57] In other words, organizations

---

[50] Data Protection Directive, *supra* note 8, at art. 4(1)(a).
[51] Data Protection Directive, *supra* note 8, at art. 4(1)(c).
[52] WP29 Opinion, *supra* note 47, at 6–7.
[53] WP29 Opinion, *supra* note 47, at 10.
[54] WP29 Opinion, *supra* note 47, at 10–11.
[55] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, at ¶¶ 55–57 (May 13, 2014).
[56] Stephan Wilske & Teresa Schiller, *International Jurisdiction in Cyberspace: Which States May Regulate the Internet*, 50 FED. COMM. L.J. 119, 175.
[57] *Google Spain*, 2014 E.C.R. 317, at ¶ 57.

engaged in moneymaking activities targeting a particular country are subject to its laws.

B. *Data Controller & Processing*

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

The CJEU found that Google is a Controller under the definition in the Directive, because Google determines the purpose and means of organizing personal data.[58] 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 . . . ."[59] With respect to the indexing of the personal data included in the results of the search queries, the CJEU 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.[60]

The CJEU spent more time analyzing whether by providing those search engine results, Google was "processing" personal data 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."[61] It found that Google is "processing data" based on its analysis that Google's

---

[58] *Id.* at ¶ 41.

[59] Data Protection Directive, *supra* note 8, art. 2(d).

[60] *Google Spain*, 2014 E.C.R. 317, at ¶ 33 ("It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing pursuant to Article 2(d).").

[61] Council Directive 95/46, art. 2(b), 1995 O.J. (L 281) (EC).

search engine does not simply transmit information but processes and organizes information to help individuals find answers to questions.[62]

The CJEU's 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.[63] The primary question is whether Google's search engine functions more like a telephone service provider[64] that simply allows the information to pass through, or more like a private investigator who helps individuals find the answers to their questions.

The merits of the CJEU's analysis of this issue are open to debate. The CJEU appears to comment on Google's indexing activities when it states:

> in exploring the internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' 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.[65]

The CJEU 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."[66] The CJEU's conclusion is also supported by the Working Party opinion on search engines, which states: "Search engines process information, including personal information, by crawling, analysing and

---

[62] *Google Spain*, 2014 E.C.R. 317, at ¶ 55 (May 13, 2014).

[63] The internet relies on a variety of hardware, software and services to allow information to be transmitted globally. If all companies who produce these products and services were held responsible for the content sent over the internet, then it would be a substantial disincentive for companies to provide these products.

[64] It is the telephone service provider's role as an information intermediary to take data from point A to point B, without modifying that data in any way.

[65] *Google Spain*, 2014 E.C.R. 317, ¶ 28 (May 13, 2014).

[66] *Id.* at ¶ 20–21 & ¶ 41.

indexing the World Wide Web and other sources they make searchable and thereby easily accessible through these services."[67]

Google's success in the marketplace has depended on its ability to accurately determine which results individuals want to see. The CJEU appears to be saying that indexing based on importance to the searcher makes the company's search engine activities function more like a private investigator and less like a telephone service provider.

The CJEU'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. In the European Union ("EU"), the controlling legal instrument on this issue is the E-commerce Directive.[68] Article 12 of the EU's E-commerce Directive addresses the definition of an information intermediary by asking whether the Internet service is acting as a "mere conduit" of the information.[69] Under this definition, the EU 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 in the results. In the *Google* case, the CJEU appears to be of the opinion that Google's use of an algorithm to index information and determine which 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, and may come to a different

---

[67] WP29 Opinion, *supra* note 47, at 13.

[68] *See* Directive 2000/31, of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') 2000 O.J. (L 178) 1 [hereinafter E-commerce Directive], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:en:HTML.

[69] *Id.* at ¶ 44 (stating that "[a] service provider who deliberately collaborates with one of the recipients of his service in order to undertake illegal acts goes beyond the activities of 'mere conduit' or 'caching' and as a result cannot benefit from the liability exemptions established for these activities").

result.[70] However, it is odd that Google has contended in their statements about the CJEU's ruling that it is an information intermediary that should not be subject to restrictions based on the information delivered through its service, and at the same time asserted that it is a speaker being censored by being prohibited from displaying the results that its algorithm determines to best respond to the query.[71]

C. *Removal of Search Engine Link*

Given the basis for the CJEU determination that Google is subject to Spanish data protection law, and that Google satisfies the definitions of "controller" and "processing" in this context, analysis turns to how the CJEU interpreted the Directive. Popular media outlets incorrectly report that the CJEU's opinion establishes a "right to be forgotten."[72] While that term describes an element of the proposed General Data Protection Regulation ("Regulation") [73] currently under consideration which would replace the Directive, the way in which the question was posed in the case created some of this confusion. For example, the Spanish Court asked the CJEU 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] the

[70] *See e.g.*, Communications Decency Act 47 U.S.C. § 230 (2015) (granting immunity to third-party publishers like search engines and service providers from libel, defamation and other privacy torts).

[71] David Drummond, *We Need to Talk about the Right to be Forgotten*, THE GUARDIAN (July 10, 2014, 5:05PM), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate ("[T]he Guardian could have an article on its website about an individual that's perfectly legal, but we might not legally be able to show links to it in our results when you search for that person's name. It's a bit like saying the book can stay in the library but cannot be included in the library's card catalogue.").

[72] *See, e.g.*, Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014) http://www.newyorker.com/magazine/2014/09/29/solace-oblivion ("The Court went on to say . . . that all individuals in the countries within its jurisdiction *had the right to prohibit* Google from linking to items that were 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed and in the light of the time that has elapsed.'") (emphasis added).

[73] *See* GDPR Proposal, *infra* note 82.

> following question is asked: 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, even though the information in question has been lawfully published by third parties?[74]

This question is a fairly straightforward request for analysis of the provisions of the Directive. However, both the language in the header, stating that the question should be evaluated in the context of *derecho al olvido* and its inclusion of a phrase about the individual asking that the information be "consigned to oblivion" (also emphasized) create an impression that the CJEU's holding is broader that it is in fact.[75]

The CJEU spends little time considering what it means to be "forgotten" or "consigned to oblivion." In fact, the CJEU's responses to the four questions referred to it do not include the words "forgotten," "forgetting" or "oblivion." The CJEU's analysis only includes these words to refer back to the Spanish CJEU's questions[76] or to reference arguments made by the parties to the case.[77] Rather, the CJEU spends the majority of its opinion describing how Mr. Costeja González's request for deletion of the links fits squarely within Article 6(1)(c) of the Directive.[78]

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."[79] The CJEU analyzes this provision of the Directive by asking what

---

[74] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, at ¶ 20 (May 13, 2014).
[75] *Id*.
[76] *Id*. at ¶ 89.
[77] *Id*. at ¶¶ 90–91.
[78] *Id*. at ¶ 72 & ¶ 92.
[79] Data Protection Directive, *supra* note 8, art. 6(1)(c).

the "further processing" of the information was in this context.[80] On this point, the CJEU applies the law quite narrowly, and states several times that it is only asking the question of which results are a relevant and proportionate response to a search query of Mr. Costeja González's name.[81] The CJEU does not determine whether those same results would have been appropriate for searches of "Costeja González real estate auction," "La Vanguardia social security debts," or "1998 real estate auctions." Given the repeated language in the opinion limiting application of the ruling only to results responding to queries of Mr. González's name, it is reasonable to think the CJEU may have decided that the linked pages at issue in the case would have been appropriate for searches specifically targeting Mr. González's real estate affairs and social security debts.

So why has this limited ruling created such a stir about a so-called "right to be forgotten?" Many legal commentators and companies have expressed concern with the EU's attempts to place a "right to be forgotten" in the General Data Protection Regulation.[82] As originally proposed by the European Commission,

---

[80] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶ 98 (June 25, 2013).

[81] *Id.*

[82] *See* Data Protection Directive, *supra* note 8, art. 17, 1995 O.J. (L 281) [hereinafter GDPR Proposal]. *See also* Miquel Peguera, *The Shaky Ground of the Right to be Delisted*, VAND. J. OF ENT. & TECH. L. (forthcoming, 2016) (manuscript at 4, note 5) (explaining that both the European Parliament and the European Council have adopted different possible versions of the GDPR). For a comparative table demonstrating the differences between the proposals, see Council of the European Union, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, http://www.statewatch.org/news/2015/jul/eu-council-dp-reg-trilogue-10391-15.pdf [hereinafter GDPR Comparison Chart]. European lawmakers aim to have a final text at the conclusion of the trilogues period at the end of 2015. As of December 2015, regulation was still in the "trilogue" process. Trilogues are an informal part of the European Union decision making process whereby representatives from the Commission, Council of Ministers and European Parliament gather to pre-negotiate politically urgent legislation. Agreements that are borne out of the trilogues process are later ratified through the formal decision making processes of the Union. The

the GDPR would have established this right and obligated online publishers to delete sources or posted references to sites where personal data were originally posted or processed.[83] Had such a provision been implemented it might have created some type of "forgetting" or "oblivion." However, this language was widely criticized as impossible to implement and was not included in the GDPR as adopted.[84]

More recent language from the European Parliament and the Council of the European Union substantially narrowed the obligation to closely reflect the provisions in Article 6(1)(c) of the Directive.[85] While the relevant provision's title still includes the phrase "The Right to be Forgotten," the requirements created by the text are similar to those of Article 6(1)(c) of the Directive.[86]

---

purpose of the process is to find an accord on a package of amendments acceptable to both the Council of Ministers and the European Parliament. Negotiations often take about a year but can help fast-track legislation through the political process. *See, e.g.*, Christine Reh, *Is Informal Politics Undemocratic? Triologues, Early Agreements and the Selection Model of Representation*, 21 J. OF EUR. PUB. POL. 822, 829 (2014).

[83] *See* GDPR Comparison Chart, *supra* note 82.

[84] *Id.* The Commission Language stated:

> (53) Any person should have the right to have personal data concerning them rectified and a *'right to be forgotten'* where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing, and later wants to remove such personal data especially on the Internet.

Id. (emphasis added).

[85] GDPR Comparison Chart, *supra* note 83.

[86] Data Protection Directive, *supra* note 8, at art. 6(1)(c) ("Member States shall provide that personal data must be . . . adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.").

D. *The Balancing Test*

The CJEU 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.[87] The CJEU's opinion, contrary to its depiction in the media, creates a narrow, fact-based determination that sixteen-year-old real estate debts are not relevant enough in this context. The CJEU 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.[88]

However, neither the Spanish Court, nor the CJEU, required that the underlying newspaper articles should be deleted from the Internet. Interestingly, the CJEU, in a sense, said that Google's algorithm did a poor job of indexing the search results.[89] Google attempts to provide search results that are as relevant as possible for the searcher.[90] Individuals who want to know as much as possible about another person (for example, a parent searching on the name of a prospective babysitter), may view even financial data dating back sixteen years as relevant. Google's market share in Internet searching appears to indicate that the company is quite good at producing relevant results.

---

[87] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, ¶ 72 (May 13, 2014). *See also* Data Protection Directive, *supra* note 8, art. 6.

[88] *Google Spain*, 2014 E.C.R. 317, at ¶ 91 (explaining that the plaintiff "may oppose the indexing by a search engine of personal data relating to him where their dissemination through the search engine is prejudicial to him and his fundamental rights to the protection of those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.").

[89] *Id.* at ¶ 92–93.

[90] Will Oremus, *Google's Big Break*, SLATE (Oct. 13, 2013, 11:50 PM), http://www.slate.com/articles/business/when_big_businesses_were_small/2013/10/google_s_big_break_how_bill_gross_goto_com_inspired_the_adwords_business.html.

The CJEU's opinion raises additional questions. Even if some search results are deemed relevant, when would these results 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 CJEU to fully examine them. Instead, the CJEU appears to rely upon the facts that the newspaper articles were sixteen years old and were not currently relevant to a search of Mr. Costeja González's name.

This case suggests consideration of a hypothetical Internet company called www.spyonyourneighbor.com, and whether privacy legislation should prohibit the use of personal data to spy on individuals. It may be that the business of www.spyonyourneighbor.com is not hypothetical at all, but rather an aspect of the way search engines function. The CJEU addressed this 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.[91] While this ruling 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.[92] The result is, therefore, much more about obscurity than it is about a right to be forgotten. The ruling has the effect of obscuring information from searches solely based on a name, when the search results are irrelevant or excessive. The author has also written about the value of using obscurity to protect privacy.[93] And

---

[91] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶ 48 (June 25, 2013) ("An internet search engine service provider may automatically acquire personal data relating to its users . . . .").

[92] For an explanation of "relevancy requirement," *see supra* notes 74–76 and accompanying text.

[93] David Hoffman, *How Obscurity Could Help the Right to Fail*, POLICY @ INTEL BLOG (Mar. 13, 2013) https://blogs.intel.com/policy/2013/03/29/how-obscurity-could-help-the-right-to-fail/ (explaining that obscurity is a rational

for those who incorrectly assume these concepts of relevance and obscurity are only European or theoretical, one commentator has described both how these important concepts form the basis for some of the United States' most effective privacy legislation, the Fair Credit Reporting Act.[94]

E. *Comparing* Google Spain *to European Court of Human Rights Free Expression Jurisprudence*

This section looks to the European Court of Human Rights ("ECHR") case law for principles for evaluating conflicts between privacy and free expression. Critical to any analysis of the *Google Spain* opinion is its impact on free expression. The Charter of Fundamental Rights not only includes Articles 7 and 8 as mentioned above, but also Article 11: the Right to Freedom of Expression and Information.[95] The Charter's Article 11 was largely based on the Council of Europe's Convention on Human Rights Article 10.[96]

---

desire because individuals need "a sphere of privacy where they know they can make mistakes, without those errors following them for the rest of their lives").

[94] Martin Abrams, *Context & Balance*, THE INFO. ACCOUNTABILITY FOUND. BLOG (Jul. 14, 2014), http://informationaccountability.org ("Many have argued that the limits built into the FCRA [Fair Credit Reporting Act] are an abuse of free expression. However, the context is a societal value that old payment data should not affect employment, credit, or insurance.").

[95] European Charter, *supra*, note 21, art. 11, (Freedom of expression and information) states:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers;
>
> (2) The freedom and pluralism of the media shall be respected.

Id.

[96] European Convention, *supra* note 31, at art. 10. Article 10 of the European Convention on Human Rights states:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions,

The CJEU's minimalist mode of analysis and opinion writing provides little clarity with respect to many of the legal issues in *Google Spain*, among them how to balance privacy against freedom of expression.[97] A curious CJEU omission is an analysis of ECHR case law on this point. As one commentator noted, "[T]he judgment appears to dismiss important considerations that can conflict with the right to be forgotten, such as the rights of freedom of expression and access to information . . . ."[98] The ECHR is no stranger to data protection and privacy law issues, therefore it is puzzling that the CJEU chose not to look to some of the ECHR's cases.[99] Three cases have been brought before the ECHR that are directly on point, namely *Axel Springer AG v.*

> restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

Id.

[97] Other commentators have criticized the CJEU's balancing approach in *Google Spain*. *See e.g.*, Christopher Kuner, *The Court of Justice of the EU Judgment on Data Protection and Internet Search Engines*, 3/2015 LONDON SCHOOL OF ECON. AND POL. SCI. (LSE) LAW, SOCIETY, AND ECONOMY WORKING PAPER SERIES 1, http://ssrn.com/abstract=2496060; Eleni Frantziou, *Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, Google Spain, SL, Google Inc v Agencia Espanola de Proteccion de Datos*, 14 HUMAN RIGHTS L. REV. 761 (2014); Michael L. Rustad and Sanna Kulevska, *Reconceptualizing the Right To Be Forgotten To Enable Transatlantic Data Flow*, 28 HARV. J.L. & TECH. 349 (2015).

[98] FRANTZIOU, *supra* note 97, at 762.

[99] Cross-references between the two CJEUs have been increasing over time, reaching over 57 mentions in 2011. Elena Butti, *The Roles and Relationship between the Two European CJEUs in Post-Lisbon EU Human Rights Protection*, JURIST (Sept. 12, 2013), http://jurist.org/dateline/2013/09/elena-butti-lisbon-treaty.php.

Germany,[100] *Von Hannover v. Germany,*[101] *and Węgrzynowski & Smolczewski v. Poland*.[102]

Axel Springer AG and *Von Hannover* were two cases involving well-known public figures attempting to enjoin media outlets from publishing (potentially) damaging information about their private lives.[103] The ECHR in both instances articulated a detailed test to provide guidance on how to evaluate the tension between free expression (Article 10) and privacy (Article 8).[104] In both judgments, the ECHR explains that, "Where the right to freedom

---

[100] 2012 Eur. Ct. H.R. 227, http://hudoc.echr.coe.int/eng?i=001-109034.

[101] (No. 2), 2012 Eur. Ct. H.R. 228, http://hudoc.echr.coe.int/eng?i=001-109029.

[102] Wegrzynowski & Smolczewski v. Poland, 2013 Eur. Ct. H.R. 224, *available at* http://hudoc.echr.coe.int/eng?i=001-122365.

[103] *Axel Springer AG*, 2012 Eur. Ct. H.R. 227 at ¶¶ 9–15; *Von Hannover*, 2012 Eur. Ct. H.R. 228 at ¶¶ 10–15.

[104] European Convention, *supra* note 31. Art. 8 (Respect for private and family life) states:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Id.

Art. 10 (Freedom of expression) states:

> (1) Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.
>
> (2) The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

European Convention, *supra* note 31. Art. 10.

of expression is being balanced against the right to respect for private life, the criteria laid down in the case-law that are relevant to the present case are set out" in a six-point test.[105] The test requires the ECHR to examine: (1) contribution to a debate of general interest; (2) how well-known is the person concerned and what is the subject of the report; (3) prior conduct of the person concerned; (4) method of obtaining the information and its veracity/circumstances in which the [media] was published or acquired; (5) content, form, and consequences of the publication; and (6) the severity of the sanction imposed by the local courts.[106] The interplay of the values underlying Article 8 and Article 10 are well expressed in elements of the six-point test. Critics of *Google Spain* might have been more satisfied with the decision had the CJEU applied a detailed analysis of the facts as seen through the lens of this test.

In *Węgrzynowski & Smolczewski v. Poland* two lawyers filed suit against an online news media website that allegedly published libelous information about them.[107] When the local court refused to hear their request to have the article removed from print, the plaintiffs filed a complaint with the ECHR, arguing that Polish Government breached their rights to respect for their private life and reputation, as protected by Article 8 of the Convention.[108] Here, the ECHR did not reiterate the Springer-Hannover test, but they did mention both cases in the decisions.[109] The ECHR expressed reservations about applying offline media regulations to the Internet, stating:

> [t]he Internet is an information and communication tool particularly distinct from the printed media, especially as regards [to] the capacity to store and transmit information. The electronic network, serving

---

[105] *Von Hannover*, 2012 Eur. Ct. H.R. 228 at ¶ 108. *See also Axel Springer*, 2012 Eur. Ct. H.R. 227 at ¶ 89.

[106] *Von Hannover*, 2012 Eur. Ct. H.R. 228 at ¶ 108.

[107] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶¶ 6–7 (June 25, 2013).

[108] *Id.* at ¶¶ 11–21. The lawyers filed suit at the ECHR against the Polish government because the Warsaw Regional Court, Court of Appeals, and Supreme Court refused to hear the case.

[109] *Id.* at ¶¶ 56–57.

> billions of users worldwide, is not and potentially will never be subject to the same regulations and control.[110]

The ECHR went on to explain that it "accepts that it is not the role of judicial authorities to engage in rewriting history by ordering the removal from the public domain of all traces of publication which have in the past been found . . . ."[111] Here, too, critics of the *Google Spain* judgment could point to the *Węgrzynowski & Smolczewski* decision for the argument that it was not the role of the CJEU to enable a revision of historically truthful data by requiring suppression or erasure.[112] But finally, as in *Google Spain*, the ECHR in *Węgrzynowski & Smolczewski* recognizes "the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press."[113] Therefore, despite the ECHR's dicta about the importance of the internet and the free flow of data, the *Węgrzynowski & Smolczewski* case is not so different from the *Google Spain* ruling that recognizes the possibility of protecting privacy when there is only limited impact on the freedom of expression.

Given the direct applicability of these cases, it is unfortunate that the CJEU did not include analysis of the relevant ECHR case law in the *Google Spain* decision. If the CJEU had looked to the ECHR cases it likely would not have issued a different ruling; however, it would have provided more clarity about the extent to which the ruling should be applied to different facts.

Let us suppose that the CJEU adopted the Springer-Hannover test. Google's processing of Mr. Casteja González's data would fail this test, as publication of sixteen-year old fully repaid debts from a non-public figure is not critical for the preservation of free

---

[110] *Wegrzynowski & Smolczewski*, 2013 Eur. Ct. H.R. 224, at ¶ 58 (quotations omitted).

[111] *Id.* at ¶ 65.

[112] Critics may also point to Frantziou, *supra* note 97 at 774 (noting that while the *Google Spain* case is not necessarily incompatible with the ECHR, the ECHR's judgment in *Węgrzynowski and Smolczewski* suggests that such incompatibility cannot be ruled out either.).

[113] *Wegrzynowski & Smolczewski*, 2013 Eur. Ct. H.R. 224, at ¶ 58.

expression. Nevertheless, such analysis is valuable and would have provided useful guidance for businesses, policymakers, and academics. The *Google Spain* Advocate General's report warned the CJEU that asserting the existence of a right to be forgotten or any similar iterance of such a right would be problematic. It stated that enforcement of a right to be forgotten would call into question its compatibility with other fundamental rights, already inked into the Charter.[114] The lack of explanatory guidance in the CJEU opinion created the uncertainty the Advocate General warned against.

In the following sections, the paper explores this global uncertainty and recommends how to move forward with implementation that would establish criteria for decisions about delisting, enhance legal certainty for companies making these decisions, and minimize the impact on free expression.

V. IMPLEMENTATION OF *GOOGLE SPAIN*: GLOBAL IMPACT

The effects of the *Google Spain* decision and the "right to obscurity" have reverberated worldwide, causing organizations to rethink the complex issues surrounding privacy and freedom of expression.[115] Individuals around the world express concern about the degree to which people can access information about them, while they increasingly use Internet tools to discover information about others (job candidates, child care givers, prospective romantic partners, neighbors, teachers, etc.). Policymakers worldwide are re-examining the degree to which individuals should be able to "know" each other. Countries such as France, Canada, Russia, Hong Kong and South Korea are attempting to determine how much access to information about individuals is appropriate.[116]

---

[114] Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424, ¶ 81 (June 25, 2013).

[115] Phil Muncaster, *Firms Already Swamped by Right to be Forgotten Requests*, INFOSECURITY, www.infosecurity-magazine.com/news/firms-swamped-right-to-be.

[116] *See infra* parts V.A–G.

In an age of easy access to sensitive personal information, countries' interest in fostering individuals' obscurity is understandable. Search engines and data brokers have quantitatively and qualitatively changed the ability to access information about individuals, no matter how private, and no matter what the potential risk the information creates. Access to information is now global—anyone on the planet can instantly probe the details about a person located anywhere around the world. This unprecedented access to the details of others' lives highlights the conflicting way varying cultures view governments' need to protect citizens from harm and from observation by others.[117]

Countries are responding to this issue in a variety of ways. Some countries are attempting to enforce delisting requests beyond EU borders.[118] Other non-European countries are weighing the consequences of introducing their local flavor of obscurity into their Internet, data protection, and cyber security laws.[119] What follows are examples of how different countries are dealing with the issue.

A. *France*

In Europe, issues surrounding data protection, privacy and freedom of expression do not end with the CJEU decision. Many post-*Google Spain* challenges remain, in particular for member states who must address citizens' concerns about data protection, erasure, obscurity, and freedom of expression.[120] The Article 29 Working Party issued guidelines asserting that, "Under EU law, everyone has a right to data protection . . . . Decisions must be

---

[117] For an excellent book discussing these developments, see VIKTOR MAYER-SCHONBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (Princeton Univ. Press, 2011).

[118] Samuel Gibbs, *French Data Regulator Rejects Google's Right-to-be-Forgotten Appeal*, THE GUARDIAN (Sept. 21, 2015), www.theguardian.com/technology/2015/sep/21/French-google-right-to-be-forgotten-appeal.

[119] *See infra* Part V.

[120] Jeff J. Roberts, *Google Defies France over "Right to be Forgotten,"* FORTUNE (Jul. 30, 2015), http://fortune.com/2015/07/30/google-france-right-to-be-forgotten/.

implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented."[121] Although the opinions issued by the working group are non-binding, they can be influential. The French privacy regulators appear to have found this language particularly persuasive, given the French regulator's subsequent engagements with Google. Since the ruling was handed down, France has been at the forefront of this dialogue and the post-decision implementation process.

In June 2015, *La Commission National de l'Informatique et des Libertes* ("CNIL"),[122] the French privacy regulatory body, ruled that Google was required to abide by "obscurity" requests in France, not only locally, but globally.[123] Although the search engine automatically directs users in France to Google's French domain (google.fr) by analyzing the location of the connecting Internet protocol address, French citizens are still able to access Google's other international domains (e.g., google.com, google.ca). At first, the CNIL's orders mirrored the CJEU ruling in that the CNIL's removal requests were specific to the Google France domain.[124] However, cognizant of the fact that users around the world can easily redirect their search inquiries to other Google sites, the CNIL sought to prevent users from accessing the

[121] Mark Scott, *France Wants Google to Apply Right to Be Forgotten Ruling Worldwide of Face Penalties*, N.Y. TIMES (June 12, 2015), http://bits.blogs.nytimes.com/2015/06/12/french-regulator-wants-google-to-apply-right-to-be-forgotten-ruling-worldwide/.

[122] CNIL's purpose, generally, is to educate its citizens about impending privacy issues, to protect its citizens from privacy and civil liberty harms, to regulate issues dealing with privacy and the digital economy, and to penalize those that violate French privacy rules. CNIL is the administrative body responsible for enforcing the erasure requests. *See* Role and Responsibilities, CNIL, https://www.cnil.fr/en/cnils-missions.

[123] *See CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine*, CNIL (June 12, 2015) *http://www.cnil.fr/linstitution/actualite/article/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/* ("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.").

[124] *Id.*

suppressed information at any and all access points.[125] In their view, to do otherwise would render a removal order ineffective.[126]

French authorities gave Google two weeks to apply the ruling across all of its domains or face fines of over $350,000.[127] The company appealed the CNIL's ruling.[128] But in September 2015, the CNIL rejected Google's effort to limit the worldwide application of the ruling for French applicants or face financial penalties.[129] Any potential fine will be appealed in French courts.[130] Google's appeal to the CNIL was rejected largely because of the regulator's concern about the ease with which the right to obscurity could be circumvented.[131]

The CNIL attempted to mitigate concerns about its worldwide removal request by explaining that any information sought can still be accessed at its original sources and that removal of the information is not absolute.[132] However, it appears that the CNIL is not just worried about citizens in France seeing the non-relevant material. Instead, it seems the CNIL wants to make certain that no one in the world is able to do an Internet search to reveal the information.[133]

It remains to be seen whether Google will propose to the CNIL alternative ways to carry out its orders, such as by increasing the degree to which it blocks access to other Google domains inside of

---

[125] *Id.*
[126] *Id.*
[127] Commission Nationale de L'Informatique et des Libertes, *CNIL Orders Google to Apply Delisting on All Domain Names of the Search Engine*, CNIL (June 12, 2015), http://www.cnil.fr/linstitution/actualite/article/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/.
[128] *Id.*
[129] Mark Scott, *France Rejects Google's Efforts to Limit Application of Privacy Ruling*, N.Y. TIMES (Sept. 21, 2015), http://bits.blogs.nytimes.com/2015/09/21/france-rejects-googles-efforts-to-limit-application-of-privacy-ruling/.
[130] *Id.*
[131] Commission Nationale de L'Informatique et des Libertes, *Right to Delsiting: Google Informal Appeal Rejected*, CNIL (Sept. 21, 2015), http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/.
[132] *Id.*
[133] *Id.*

France. Google could accomplish this by preventing users from manually overriding the selection of Google.fr. Individuals could still use other methods, such as spoofing IP addresses[134] from other geographies to access Google.com. Moreover, it is unclear the extent to which the CNIL would force Google to silo its services geographically, and the degree to which French CJEUs would continue to find jurisdiction over those non-French domains. Also, as mentioned above, none of these efforts will accomplish the CNILs goal to protect French citizens from people accessing information outside of France. This conflict is one that many Internet companies will likely face as they attempt to provide global services that conflict with local laws and cultures.[135] Implementation challenges are not unique to the European continent. France is just one example.

B. *Other EU Member States*

The Spanish implementing legislation requires that the Spanish court now issue its own ruling in accordance with the CJEU opinion. Similarly, each individual EU Member State data protection authority will need to interpret the opinion as they apply their national laws. The fragmentation that will result from the application of twenty-eight member state laws will pose serious compliance problem for global companies. The CJEU held that data from sixteen years ago is too old to be relevant in the context of the facts of the *Google Spain* case.[136] How does a court determine at what point or under what circumstances data is no longer relevant? It is difficult to predict how twenty-eight different

[134] In computer networking, Internet Protocol ("IP") address spoofing or IP spoofing is the creation of IP packets with a forged source IP address, with the purpose of concealing the identity of the sender or impersonating another computing system. *See IP Spoofing*, CISCO.COM, http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_10-4/104_ip-spoofing.html.

[135] *See, e.g.*, Peter Fleischer, *Implementing a European, Not Global, Right to be Forgotten*, GOOGLE EUROPE BLOG (July 30, 2015), http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html.

[136] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014 E.C.R. 317, ¶ 98 (May 13, 2014).

member states will interpret the need to optimize the rights of the individual and the "preponderant interest of the general public . . . ."[137]

The CJEU is not charged with addressing concerns about harmonization, and its decision creates a pressing need for further guidance. It also points to one of the problems posed by the European system in which the Directive creates a regulatory floor, but not a ceiling for member states. The case illustrates why it is important to further pursue harmonization mechanisms 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 certainty across Europe.[138]

C. *Canada*

The British Columbia Supreme Court in Canada dealt with the issue of the ability of Internet search engines to provide global access to information, and how privacy and freedom of expression should be balanced. In *Equustek Solutions, Inc.* v. *Datalink Technologies, Inc.*,[139] an appellate court in British Columbia required Google to remove sensitive intellectual property information from the results provided by all of its local and international search engines.[140] In *Equustek*, the complaining company filed suit against a hardware distributor for distributing Equustek products under its own name.[141] The underlying case was a fairly uncontroversial Canadian trademark infringement case to which Google was not a party. Equustek applied to the British

---

[137] *See* Press Release No 70/14, *supra* note 1.

[138] *See generally The One-Stop-Shop Mechanism*, COUNCIL OF THE EU 6833/15 (2015), http://register.consilium.europa.eu/doc/ srv?l=EN&f=ST%2068 33%202015%20INIT (discussing how the GDPR Proposal's "One-Stop-Shop" was created in hopes of providing for more uniformity in data protection enforcement. The mechanism is supposed to allocate responsibility for supervising data controllers and data processors that are working in several different European markets to a "main establishment" so that it eliminates the complexities of having to work with a different data protection authority in whatever jurisdiction the controller or processor operates).

[139] Equustek Sols. Inc. v. DataLink Technologies, [2014] BCSC 1063 (Can.).

[140] *Id.* at ¶ 9 (Can.).

[141] *Id.* at ¶¶ 4–5.

Columbia Supreme Court for an injunction ordering Google to remove all links to Datalink websites from all searches conducted worldwide.[142]

There is precedent in Canadian law for issuing interlocutory orders to protect Canadian companies from further trade secret or intellectual property rights violations.[143] Therefore, the fact that Google was not a party to the underlying litigation did not prevent the court from making the order.[144] Google claimed that the injunction should not have been granted because (1) the application did not have a sufficient connection to the Province to give the Supreme Court of British Columbia competence to deal with the matter and (2) "the extraterritorial reach of the injunction is inappropriate and a violation of the principles of comity."[145] The Supreme Court granted the injunction, because it was sympathetic to the plaintiff's argument that effective protection of its trademark would require global obscurity so that it could be properly protected.[146]

As in France, the *Equustek* court advocated for worldwide removal of specific information from all Google domains.[147] The court found a "real and substantial connection" between Google and British Columbia through Google's advertising activities, using an analysis similar to that in *Google Spain*.[148] Even though Google houses no servers or offices in British Columbia, the court found that the company had purposefully availed itself of Canadian territory and thus should be subject to *in personam* jurisdiction.[149] Advertising, the use of web crawler software, and similar business

---

[142] *Id.* at ¶¶ 8–9.

[143] *See* Equustek Sols. Inc. v. Google Inc., [2015] BCC 265, ¶ 69 (Can.); *see also* judgment of Arnold J. in *Cartier International AG v. British Sky Broadcasting Limited* [2014] EWHC 3354 (Ch.) (Plaintiffs were granted injunction order against a large number of British ISPs requiring them to block access to websites that violate trademarks.).

[144] *See* Equustek Sols. Inc. v. Jack, [2014] BCSC 1063, ¶ 2 (Can.).

[145] *Id.* at ¶ 3.

[146] *Id.* at ¶¶ 25–27.

[147] *See generally id.*

[148] *See id. at* ¶ 29.

[149] *Id.* at ¶ 54.

activities consisted of contacts sufficiently substantial to subject Google to Canadian jurisdiction.[150]

Google attempted to make an extraterritoriality argument by claiming that the court could not regulate the activities in foreign jurisdictions due to pragmatism and comity.[151] But the court explained that *in personam* jurisdiction is not limited by residency; because Google does business in Canada, it may have jurisdiction over it due to its activities.[152] The court also found that concerns about comity were overblown.[153] "The only comity concern that has been articulated in this case is the concern that the order made by the trial judge could interfere with freedom of expression in other countries."[154] The court doubted the potential of its decision to affect other nations or to conflict with the fundamental principles of other nations on freedom of expression and data protection.[155] Focusing on the intellectual property aspect of the case, the court explained that the protection of intellectual property rights should come before Google's commercial advertising business.[156] The court concluded that, internationally, it is not

---

[150] *Id.* at ¶¶ 55–56.

[151] *Id.* at ¶ 81 ("As a matter of law, the court is not competent to regulate the activities or non-residents in foreign jurisdictions. This competence limiting rules is dictated both by judicial pragmatism and considerations of comity. The pragmatic consideration is that the Court should not make an order that it cannot enforce. The comity consideration is that the Court refrains from purporting to direct the activities of persons in other jurisdictions and expects Courts in other jurisdictions to reciprocate.").

[152] Equustek Sols. Inc. v. Google Inc., [2015] BCC 265, ¶¶ 84–85 (Can.).

[153] *See id.* at ¶ 91.

[154] *Id.*

[155] *Id.* at ¶ 93.

[156] *See id.* Notably, the British Columbia Court of Appeals also cites to the *Google Spain* Case and to the controversial *Yahoo France* Case. *See e.g.*, Equustek Sols. Inc., [2015] BCC 265 at ¶¶ 95–96 ("I do not suggest that these rulings have been without controversy or problems."). *See, e.g.*, *La Ligue contre le racisme et l'antisémitisme c. La Société YAHOO!Inc.*, Tribunal de Grande Instance de Paris (May 22, 2000 and Nov. 20, 2000); YAHOO!Inc. v. La Ligue contre le racisme et l'antisémitisme, 169 F. Supp. 2d 1181 (N. D. Cal., 2001), *rev'd* 379 F.3d 1120 (9th Cir. 2004); YAHOO! v. La Ligue Contre Le Racisme, 433 F.3d 1199 (9th Cir. 2006) (en banc).

unusual for courts or regulatory bodies to issue such orders, despite their potential complexities.[157]

D. *Hong Kong*

Allan Chiang, the head privacy official of Hong Kong, has asked Google to "observe the right to be forgotten outside of Europe"[158] in the interest of protecting citizens' privacy. However, critics have expressed concern about the effect of such a policy, stating that it could encourage Hong Kong government leaders to follow the example of the People's Republic of China ("PRC") and substantially limit the free flow of information.[159] Currently information flows in Hong Kong remain relatively protected and unregulated except in instances related to media and publication rights.[160] Regulation in Hong Kong is generally designed to promote data flows.[161] Nevertheless, policymakers in Hong Kong are examining issues surrounding obscurity, freedom of expression and the cross-border flow of data in the West.[162]

E. *South Korea*

Communication regulators in South Korea are evaluating whether to introduce a "European-style" right to obscurity into Korean law.[163] South Korean law already includes substantial protections against online defamation, providing that individuals may request that libelous or defamatory information be removed

---

[157] *Equustek Sols.*, [2015] BCC 265 at ¶¶ 95.

[158] Simon Mundy, *Asia Considers 'Right to be Forgotten' Ruling Prompted by Google*, FINANCIAL TIMES (Mar. 12, 2015), http://www.ft.com/intl/cms/s/0/ade889d4-bc0e-11e4-a6d7-00144feab7de.html.

[159] *Id.*

[160] *Consultation Paper on the Regulation of Media Intrusion*, The Law Reform Comm'n of Hong Kong Sub-Committee on Privacy, 14–17, www.hkreform.gov.hk/en/docs/media-e.doc.

[161] *See* Thomas Chan, *New Hong Kong privacy chief vows to balance flow of information*, SOUTH CHINA MORNING POST (July 25, 2015), http://www.scmp.com/news/hong-kong/politics/article/1843525/new-hong-kong-privacy-chief-vows-balance-flow-information.

[162] *A Right to be Forgotten in Hong Kong?*, HOGAN LOVELLS (Aug. 2015), http://www.hoganlovells.com/files/Uploads/Documents/Newsflash_A_Right_to_be_Forgotten_in_Hong_Kong_HKGLIB01_1452118.pdf.

[163] *See* MUNDY, *supra* note 158.

from websites.[164] South Korea regulators have discussed potentially creating a new law that would allow for delisting from search results in certain circumstances.[165]

F. *Russia*

Legislators in Russia have drafted a law that would provide the right to obscurity to Russian citizens. The Russian law however, goes beyond the framework established in Europe.[166] In Europe, Google set up a procedure whereby "people could point out links they wanted removed from their own name-search results, along with an explanation of why the content was 'inadequate, irrelevant or no longer relevant.'"[167] Google generally requires applicants who request delisting to provide specific hyperlinks they wish to have removed.[168] The Russian bill requires only that applicants indicate the information they want deleted.[169]

The ECHR case law is clear that public figures enjoy only a limited right to privacy.[170] However, "the Russian version extends the right to erasure to public figures and information that is considered in the public interest."[171] Search companies may deny a request, but if the applicant appeals in court and wins, non-compliance could result in fines of over $50,000 per request.[172] Considering that Google has had hundreds of thousands of requests already within the EU, search engines face the prospect of significant fines in Russia.

---

[164] *See id.*

[165] *See id.*

[166] *See* Olga Razumovskya, *Russia Proposes Strict Online Right to Be Forgotten*, WALL ST. J. (June 17 2015), http://blogs.wsj.com/digits/2015/06/17/russia-proposes-strict-online-right-to-be-forgotten/.

[167] *Id.*

[168] *See id.*

[169] *See id.*

[170] *See, e.g.*, Wegrzynowski & Smolczewski v. Poland, 2013 Eur. Ct. H.R. 224, ¶ 57 ("The Court has also observed that the most careful of scrutiny under Article 10 is required where measures or sanctions imposed on the press are capable of discouraging the participation of the press in debates on matters of legitimate public concern.").

[171] RAZUMOVSKYA, *supra* note 166.

[172] *See id.*

G. *The United States*

The concepts explored in *Google Spain* are also covered in the United States Federal Trade Commission's ("FTC") analysis of the data broker industry.[173] The FTC specifically called out the challenges to privacy that come from data brokers that provide "people search" services.[174] 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 the fact that close matches of an individual's name may continue to appear in search results.[175]

The FTC report highlights United States regulators' concerns 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 name.[176] The FTC report points out that this concern is not new, but was a motivation for enactment of the Fair Credit Reporting Act in the 1970s.[177] It also cites this concern as the reason the Individual Reference Services Group temporarily established a self-regulatory program to provide more transparency with respect to people search services.[178] The United States has a long history of allowing for the "forgetting" of information deemed to have a disproportionate impact on the individual.[179] Most American states have laws that require the

---

[173] *See generally*, Edith Ramirez et al., *Data Brokers: A Call for Transparency and Accountability*, FED. TRADE COMM'N (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [hereinafter FTC Data Brokers Report].

[174] *Id.* at 46–49.

[175] *Id.* at 54.

[176] *Id.* at 46–49.

[177] *Id.* at 4.

[178] *Id.* at vii.

[179] *See, e.g.*, Melvin v. Reid, 112 Cal. App. 285, 292 (1931) (holding that the American justice system is supposed to grant the right of "rehabilitation of the fallen and the reformation of the criminal" and that revealing plaintiff's identity

expunging of criminal records of minors.[180] This motivation for erasure of these criminal records is evidence of a cultural belief that people should be allowed to make mistakes, suffer consequences for their decisions, but then be permitted to move on.[181]

Similarly, many states are pursuing "revenge porn" laws.[182] These laws would provide individuals with the ability to block the posting of explicit videos and pictures often made available by ex-lovers who want to embarrass and inflict emotional pain on their former partners. While these videos are "truthful data," often recorded with the subject's full knowledge, the United States believes that making this truthful information available will have a disproportionate impact on the individual.[183]

---

inhibited that right); *see also* Daniel Solove, *What Google Must Forget: The EU Ruling on the Right to Be Forgotten*, LINKEDIN PULSE, (May 13, 2014), https://www.linkedin.com/pulse/20140513230300-2259773-what-google-must-forget-the-eu-ruling-on-the-right-to-be-forgotten (explaining that "the Children's Online Privacy Protection Act provides for a right to delete personal data. The Fair Credit Reporting Act restricts the ability of consumer reporting agencies to report on bankruptcies and criminal proceedings that are beyond a certain number of years old"). *But see* Sidis v. F-R Publishing Corp., 113 F.2d 806 (2d Cir. 1940) (holding that one cannot easily ignore one's status as a celebrity or a public figure and thus attempt to control the dissemination of factual information about one's life despite already being a public figure).

[180] "[Forty-five] states and the District of Columbia provide for expungement for some ex-offenders or other similar relief." *Expungement*, ELECTRONIC PRIVACY INFORMATION CENTER, https://epic.org/privacy/expungement/#federal (last visited Feb. 13, 2015)

[181] Meg Leta Ambrose et al., *Seeking Digital Redemption: The Future of Forgiveness in the Internet Age*, 29 Santa Clara High Tech. L.J. 99, 110–17 (2012).

[182] Currently, twenty-six states have "revenge porn laws". *See 26 States Have Revenge Porn Laws*, END REVENGE PORN FOUNDATION, http://www.endrevengeporn.org/revenge-porn-laws/ (last visited Feb. 13, 2015) (providing citations for the applicable state law civil or penal code provision).

[183] *See, e.g.*, Michaels v. Internet Entm't Grp., Inc., et al., 5 F. Supp. 2d 823 (C.D. Cal. 1998); Amy Lai, *Revenge Porn Legislation Activists and the Lessons from Sexual Harassment Jurisprudence: Gender Neutrality, Public Perceptions and Implications*, 40 THE HARBINGER 52, 55 (2015), http://socialchangenyu.com/revenge-porn-legislation-activists-and-the-lessons-from-sexual-harassment-jurisprudence-gender-neutrality-public-perceptions-and-implications/.

The limited ability in the United States to challenge disproportionate truthful information often leads to strange results. Take for instance the posting of the nude celebrity photos allegedly accessed by hacking mobile phones.[184] Laws exist that prohibit hacking digital devices.[185] Laws also exist that prohibit those who trespass on private property from taking unauthorized videos, phone recordings, or pictures.[186] However, prosecuting the data thief does not fully mitigate the harm to the victim if search engines and data brokers will continue to direct people to the content forever. While the hacked celebrities could not request removal of the photos based on their need for privacy, they were allowed to demand the pictures be taken down based on copyright violations.[187] The celebrities, as the photographers, owned the intellectual property rights to the photos.[188] The United States legal structure in this respect has valued intellectual property rights more than privacy rights. If the images had been illegally photographed by a third party through an open window, a hotel door peep hole or an illegally installed wireless camera, the celebrities' ability to demand obscurity of the photos would be limited.

---

[184] *See, e.g.*, Mike Isacc, *Nude Photos of Jennifer Lawrence Are Latest Front in Online Privacy Debate*, N.Y. TIMES (Sept. 2, 2014), http://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html.

[185] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2010).

[186] *See, e.g.*, The Digital Millennium Copyright Act 17 U.S.C. § 512(a)–(c)(1)(C) (2012); *see also Digital Millennium Copyright Act*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/dmca (last visited Feb. 22, 2016) (explaining how the DMCA "safe harbor" provisions protect service providers from liability by complying with "notice and takedown" procedures).

[187] Alex Fitzpatrick, *Here's How Celebs Can Get Their Nude Selfies Taken Down*, TIME MAG. (Sept. 2, 2014), http://time.com/3256732/jennifer-lawrence-selfies-copyright/ ("Jennifer Lawrence, Kate Upton, Kirsten Dunst . . . could . . . file a [Digital Millennium Copyright Act] takedown notice while they fill out the paperwork for a formal copyright on their photos, assuming they took the images of themselves. If their takedown notices are ignored, they can then sue the sites in question for copyright violation.").

[188] *Id.*

VI. THE NEED FOR A GLOBAL INTERNET OBSCURITY CENTER

Search engines have responded to the lack of obscurity rights by creating their own policies for delisting or erasure. Google states in its policies that in addition to removing content that violates copyright, it also delists depictions of child sexual abuse.[189] Google also states that it may remove the following information:

> • National identification numbers like United States Social Security Number, Argentine Single Tax Identification Number, Brazil Cadastro de pessoas Físicas, Korea Resident Registration Number, China Resident Identity Card, etc.[;]
> • Bank account numbers[;]
> • Credit card numbers[;]
> • Images of signatures[;]
> • Nude or sexually explicit images that were uploaded or shared without your consent[.][190]

Google states that it uses the following criteria to determine whether it will delist the link to the information:

> To decide if a piece of personal information creates significant risks of identity theft, financial fraud, or other specific harms, we ask:
> • Is it a government-issued identification number?
> • Is it confidential, or is it publicly available information?
> • Can it be used for common financial transactions?
> • Can it be used to obtain more information about an individual that would result in financial harm or identity theft?
> • Is it a personally identifiable nude or sexually explicit photo or video shared without consent?
>
> We apply this policy on a case-by-case basis. If we believe that a removal request is being used to try and remove other, non-personal information from search results, we will deny the request. Note: We usually don't remove information that can be found on official government websites because the information is publicly available.[191]

It appears from these policies that Google understands that it must provide some level of obscurity for individuals because of the tremendous impact its services make on the lives of those people whose data is revealed. However, the mechanism by which Google

---

[189] *See Removal Policies*, GOOGLE.COM, https://support.google.com/websearch/answer/2744324?hl=en (last visited Feb. 13, 2015).

[190] *Id.*

[191] *Id.*

makes these decisions is not transparent to those individuals or regulators.

The CJEU opinion [192] 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 limit the free flow of information more than necessary to protect individual privacy. It seems unfair, and in fact inappropriate to charge private companies like Google with developing and applying criteria to determine under what circumstances to protect an individual's right to obscurity. This type of a determination is usually reserved for a body elected by and accountable to citizens. However, the complex global need for a right to obscurity creates issues related to the jurisdiction, powers and procedures of a government body that would make these determinations.

One way to deal with the complexity of implementing the CJEU's guidance would be to establish a centralized body to handle "obscurity requests" from individuals. This could be called an "Internet Obscurity Center," overseen by regulators who would opt through their country's legislation to work with the Center. This system would allow individuals to first go to the Center with a complaint, and only resort to filing a complaint with the regulator if they are not satisfied with the result provided by the Center. Regulators could provide search engines and data brokers with protection from liability when following the direction of such a centralized obscurity center. The obscurity center could function as a co-regulatory body with companies voluntarily participating. Companies would agree to eventual oversight of the regulatory agencies, and would agree to comply with delisting recommendations made by the Center. The Center would create a more efficient system, which removes the burden of making these

[192] *See* Opinion of AG Jääskinen, case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2013 E.C.R. 424 (June 25, 2013).

determinations from each individual company and provides individuals with reasonable access to a remedy. This model would also provide an international solution and an effective forum for a transparent international dialogue on the criteria for delisting.

The obscurity center would need to make difficult judgments about when information should be obscured. However, as the authors have previously written,[193] in addition to the test articulated in the ECHR case law, other criteria can be used to determine if information should warrant obscurity. The authors suggest that the following six criteria the Center could use to evaluate obscurity requests:

Criterion	Description	Example
Lapse of time	A person did a bad thing but truly feels sorry, paid debt, and learned the lesson	A drunk driving conviction followed by 20 years of sobriety and exemplary driving
Illegally obtained data	The original collection or use of the data violated a law	Trespass, identity theft, service provider employee theft, blackmail, revenge porn, stalking
Discrimination	The likelihood an individual will be discriminated against on the basis of the information	Data based on race, ethnicity, sexual orientation
Sensitive Data	Information that the individual just doesn't want people knowing	Bank account information, social security number, health data

[193] David Hoffman, *Europe's New Right to be Forgotten: Not New and Not Forgetting*, POLICY @ INTEL BLOG (July 16, 2014), https://blogs.intel.com/policy/2014/07/16/europes-new-right-forgotten-new-forgetting/.

Taken Out of Context	Information that is misleading or creates a negative impression when taken out of its original context	Placing some punk rock lyrics in a blog about the use of profanity in music, and later the lyrics are quoted as the thinking of the individual
Individual as Victim	Information about certain crime victims	Domestic violence victims

These categories and the ECHR test would need to be refined before search engines and data brokers put them into practice globally. Which organizations would be required to abide by the obscurity center's decisions would need to be clearly articulated. However, given the concentration of internet searching and data broker activity in a few powerful players, simply applying the process to the leading companies would provide individuals with access to considerable practical obscurity.

The obscurity center could establish a board of advisors comprising globally recognized privacy and free expression experts to help refine the decision-making criteria. The criteria could and should be created in an open and transparent process with full opportunity for comment by civil society, government and industry. If companies or individuals are not satisfied with any individual decision made by the obscurity center, they could appeal the decision to their country's regulator or court system. Such a system would take the burden off of the search engines and data brokers and appropriately place it on regulators and the courts.

VII. CONCLUSION

In light of the provisions of the Directive, the CJEU was neither insane, nor nearsighted when it decided *Google Spain*. It is fair, however, to fault the CJEU for providing only minimal guidance on how to implement such an important ruling on a topic critical to fundamental human rights. The CJEU's opinion has furthered a discussion that requires more analysis and creative thinking about how to promote the trust of individuals in the use of the digital infrastructure. Finding methods to implement the

CJEU's opinion will be difficult, and must guard against unduly limiting free expression.

This implementation needs to comprehend where technology is headed, given advances in data analytics, cloud computing and the Internet of things. Traditional spaces of increased privacy protection, like the home, will need these obscurity rights to continue to be a place of refuge for individuals. At the same time, the decision should be implemented in a way that will promote free expression, providing assurances that individuals can take risks, voice unpopular opinions, engage in political dissent, and question the status quo without fear that a record of their speech will be globally available in perpetuity. Continued discussion of "the right to obscurity" is necessary. That exploration is critically important at a time where efforts are underway to put in place new privacy laws around the world.