The Right to Be Forgotten: An Overview of the Evolving Global Landscape

By Francoise Gilbert[αβχ]

Francoise Gilbert is the founder and Managing Director of the IT Law Group (www.itlawgroup.com), a niche law firm that focuses on US and global information privacy and security, data governance, cloud computing, big data and other emerging technology issues. She is the author of the two-volume treatise Global Privacy and Security Law, www.globalprivacybook.com (Aspen Publishers/Wolters Kluwer Law and Business), which analyzes the data protection laws of 68 countries across all countries. Ms. Gilbert can be reached at fgilbert@itlawgroup.com or at +1-650-804-1235.

We are being told repeatedly that individuals have no interest in privacy. Advertisers, marketers, and others companies that benefit from advertising revenues argue that most people will give away very personal details in exchange for a t-shirt. This may have been true when consumers did not understand the consequences of their disclosures. This state of ignorance or naiveté is changing.

On a global basis, individuals are becoming aware of the financial and strategic value of their personal information. They know that, before offering employment or a loan, their counterpart is likely to run an online search to obtain articles, blogs, posting, photographs, or other small pieces of information. These many pieces of information might be used to sketch their profiles,

---

β *A prior version of this article was published in the February 2015 issue of the Journal of Internet Law. For copies of that article, please contact Francoise Gilbert at fgilbert@itlawgroup.com or +1 650-804-1235.*

χ *Special thanks to Joanne Kirk for her contributions to this article.*

evaluate their background or assess their reputation. In turn, this knowledge is likely to cause significant decisions to be made about them - without their input -, such as whether to offer a job, or extend a loan. Thus, it is important that these search results provide information that is current, accurate, complete, and relevant.

Until recently, individuals have unsuccessfully attempted to obtain the removal of links to articles relating to their past.[1] In the past few years, the legal and judicial landscape has evolved significantly, opening the door to requests by individuals for the removal or blocking of certain information that is likely to damage their reputation. Legislators, globally, are showing greater interest in the issue, and a greater awareness of the means in which reputations are built, or destroyed, in the Internet and social media era.

For the past three years, the European Union has been debating the conditions for the exercise of a "Right to be Forgotten" or "Right of Erasure," which is expected to be part of the final draft of the EU Data Protection Regulation. In the United States, a new California law grants minors a "Right of Erasure." Since January 1, 2015, California residents under 18 years of age have had the right to obtain the removal of any information or content that they may have provided to a site or service online.

The judicial branch also is paying attention to the complexity of the matter. In May 2014, the Court of Justice of the European Union (CJEU) granted a Spanish citizen the "right to be forgotten" and required Google to remove certain links from search results that led to information about the individual's past financial troubles that occurred more than 10 years ago.

Since the publication of the CJEU opinion, search engines have been flooded by delisting requests. As of March 2015, Google had received more than 230,000 delisting requests from

[1] See, e.g., Raffaele Zallone, The Privacy Paradox, available at *https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1116/1516.*

EU residents, and evaluated more than 831,000 URLs.[2] So far, there is less information about similar requests made with the other search engines.

The CJEU decision has caused a ripple effect on a global basis. Cases similar to the Spanish case are being filed against search engines throughout the world. For example, in Japan, in another case against Google, a Tokyo District court, presented with a request to remove search results that were hinting at past criminal activity, ruled in favor of the individual seeking the removal. A similar case was filed in Mexico.

These recent events raise many issues, such as what should be done when individuals request the removal or de-listing of information that may affect their reputation. Who should receive such requests? When and how should they be implemented? Is de-listing acceptable or appropriate? If information is no longer available due to de-listing, what is the effect on Freedom of Information? These questions will be examined in the last part of this article, after an analysis of the historical perspective and an overview of the current legal and judicial landscape.

I. Historical Perspective

Defamation, Slander, Libel

The concept of a right to a good name or reputation is not new. Laws and courts have addressed defamation claims for several centuries. Early examples of libel cases are found in England in the 17th century. In the United States, the famous Zenger Trial, in 1735, addressed the liability of a newspaper publisher who was charged with seditious libel.[3] In France,

[2] Information as of March 12, 2015. Available at *http://www.google.com/transparencyreport/removals/europeprivacy/*.

[3] See, e.g., The Trial of John Peter Zenger, *http://www.ushistory.org/us/7c.asp.*

defamation has been regulated since 1881 by the Law on the Freedom of the Press.[4]

The United States distinguishes libel (written defamation) from slander (oral defamation) and treats both as a tort. Courts have often struggled to define a proper balance between competing interests. On one hand, people should be able to speak freely; while on the other, people should not harm others by telling lies or making inaccurate statement. When considering cases regarding libel or slander, the courts have found that some people, due to their role in public life, are entitled to less protection than that afforded to private citizens, i.e. that there is a vested and legitimate public interest in the information relating to that individual. This has been the case, for example, for public figures such as politicians.

Fair Credit Reporting Act

The concept that a reputation is a valuable asset that deserves protection is also found in situations other than libel and slander. It was determined long ago that information contained in databases or resulting from the compilation of data could affect a person's reputation. The financial industry was one of the first to realize that the advent of technology and the availability of storage and data processing facilitated the creation of large databases of personal information that could be used for the determination of people's credit worthiness. It became clear that the information contained in these databases could significantly harm individuals if there was not a proper balance. As a result, in 1970, the United States passed the Fair Credit Reporting Act (FCRA),[5] to define rules for the collection, dissemination, and use of consumer information for credit purposes.

Among other things, FCRA regulates how long negative information may be retained in a consumer's file. In many ways, this is essentially a relevancy requirement, ensuring that

---

[4] Law of July 29, 1881, on the Freedom of the Press. *http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000877119.*

[5] Codified as 15 USC §1681.

information that is obsolete, or no longer relevant, does not remain in a consumer's credit report or impact future credit decisions. For example:

- Information about bankruptcy may not be used in a credit report after 10 years;[6]
- Information about civil suits, civil judgments, and record of arrest may not be used after 7 years;[7]
- Information about paid tax liens may not be used after 7 years;[8] and
- Information about accounts placed for collection or charged to profit and loss may not be used after 7 years.[9]

This right of relevancy, although clearly not legally enumerated as a specific right of the consumer in FCRA, is conceptually quite similar to the crux of the *Costeja* decision (discussed below), that a data subject has the right to request the removal of links to information that is "inaccurate, inadequate, irrelevant or excessive," even if the information is truthful. Both the FCRA and the *Costeja* case acknowledge that information that is correct and relevant at one time may, due to the passage of time, later become no longer relevant.

EU Data Protection Directive 95/46/EC

In the European Union, the EU Data Protection Directive 95/46/EC, which is the still the basis for the data protection laws of the 31 members of the European Economic Area, also recognized that it was necessary to put limits on the ability to collect and use personal data. Articles 6 and Article 12 of the 1995 Directive limit the retention of personal data, and require the blocking of incomplete or inaccurate data.

Article 12(b) requires that the national data protection laws of the EU Member States grant individuals the right to obtain from data controllers, "the rectification, erasure, or blocking of data the

[6] 15 USC §1681c(a)(1).
[7] 15 USC §1681c(a)(2).
[8] 15 USC §1681c(a)(3).
[9] 15 USC §1681c(a)(4).

processing of which does not comply with the provisions of [the] Directive, in particular because of the incomplete or inaccurate nature of the data".

In addition, Article 6 limits the retention of personal data. It requires that the national data protection laws of the EU Member States provide that personal data must be "kept in a form that permits identification of data subjects for no longer than is necessary for the purpose for which the data were collected, or for which they are further processed."

The common law of libel and slander, the Fair Credit Reporting Act, the 1995 EU Data Protection Directive and other similar laws, globally, have paved the way to the development of a legal framework where information, written or spoken, on paper or electronic, published or compiled, cannot be collected, used, distributed, retained, or used for a purpose other than the original purpose without proper concern for the adverse consequences for the individual who might be the subject of such information or compilations. It would, therefore, be inaccurate to qualify recent events, which are discussed below in this article, as coming as a surprise.

II. Existing or Proposed Legislation

In the past few years, the legal and judicial landscape regarding an individual's right to have certain information blocked or erased has evolved significantly. In Europe, the different drafts of the European Union Data Protection Regulation incorporate a "Right to be Forgotten" or "Right of Erasure." In the United States, since January 1, 2015, the California "Right of Erasure" law allows California residents under 18 years of age to obtain the removal of any information or content that they may have provided to a site or service online.

Proposed EU Data Protection Regulation

Although the national laws implementing the 1995 EU Data Protection Directive provided for a right of erasure or blocking, the concept was seldom invoked. Actions for the

blocking or erasure of content, if any, were conducted quietly, and generally were unsuccessful. The individuals' rights were limited to a right to request the erasure[10] or blocking of their own data that were inaccurate or incomplete.[11] Requests for blocking of search results that linked to material that was obsolete or no longer relevant were generally ignored.[12]

A more advanced perspective, introducing the "Right to be Forgotten," was laid out in the 2012 draft of the proposed EU General Data Protection Regulation.[13] Article 17 of the 2012 draft, provided that individuals should have the right to have personal data concerning them rectified and a "Right to be Forgotten" when the retention of such data is not in compliance with the principles set forth in the Regulation. The proposed provision would have granted individuals the right to have their personal data erased and no longer processed, when the data are no longer necessary in

---

[10] Directive 95/46/EC Article 12(b) requires that the data protection laws enacted by each Member State guarantee each individual the right to obtain from the data controller, as appropriate, the rectification, erasure or blocking of data the processing of which does not comply with the Directive, in particular because the data are incomplete or inaccurate. Directive 95/46/EC Article 12(c) also requires that the data protection laws enacted by each Member State guarantee each individual the right to obtain from the data controller that the third parties to whom the data have been disclosed be notified of any rectification, erasure or blocking carried out unless this proves impossible or involves a disproportionate effort.

[11] Directive 95/46/EC Article 6(d) provides that data that are inaccurate or incomplete, having regard to the purposes for which they were collected, or for which they are further processed must be erased or rectified.

[12] See, e.g., Raffaele Zallone, The Privacy Paradox, available at *https://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1116/1516.*

[13] On the 2012 draft of EU General Data Protection Regulation, *see http://www.itlawgroup.com/resources/articles/72-proposed-eu-data-protection-regulation-january-25-2012-draft-what-us-companies-should-know.*

relation to the purposes for which the data are collected or processed, or if the individuals withdraw their consent or object to the processing of personal data concerning them, or when the processing of their personal data otherwise does not comply with this Regulation. The proposed Article 17 allowed exceptions such as: when the data are necessary for historical, statistical and scientific research purposes, or for exercising the right of freedom of expression, or when required by law, or when there is a reason to restrict the processing of the data instead of erasing them.

Three years later, the text of the EU Data Protection Regulation is still being discussed. The concept of "Right to be Forgotten" or "Right of Erasure" is still alive in Article 17 of the draft Regulation, but it has evolved slightly as a result of much lobbying and negotiations. In addition to the intense lobbying by search engines and other data brokers, the Member States have voiced significant reservations. For instance, Germany, Denmark, and Spain, have stated that they are concerned about introducing a right that would go beyond the right to obtain from the data controller the erasure of one's own personal data. Other countries, for example, France and Belgium, have pointed out that it would be difficult to implement these provisions with respect to data posted on social media. Luxembourg, Netherland, Portugal, and the United Kingdom, among others, have commented that the "Right to be Forgotten" should be balanced against the right to remember and to have access to information sources as part of the freedom of expression.

The most recent version of Article 17, "Right to be Forgotten and to Erasure", in the revised version of the Draft General Data Protection Regulation, No. 15395/4 of December 2014 (EU Council Version), if implemented, would grant an individual the right to obtain the erasure of personal data without undue delay when one of the following grounds applies:[14]

- The data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

[14] EU Council Version, Article 17(1).

- The data subject withdraws the consent on which the processing is based, and there is no other legal ground for the processing of the data;
- The data subject objects to the processing of personal data and there are no overriding legitimate grounds for the processing;
- The data have been unlawfully processed; or
- The controller must erase the data to comply with its own legal obligations.

The exceptions to this obligation have been expanded from the initial 2012 draft. The concept and manner in which the "Right to be Forgotten" requests would be analyzed is slowly taking shape. In the EU Council version of the proposed Regulation, the obligation to erase data would not apply to the extent that access to the personal data at stake is necessary for:

- Exercising the freedom of expression;
- Compliance with a legal obligation;
- Reasons of public interest;
- Historical, statistical, and scientific purposes; or
- The establishment, exercise, or defense of legal claims.

The first and most important exception has to do with the protection of the freedom of expression. Indeed, one of the major concerns voiced about the "Right to be Forgotten", is that it might trump freedom of expression and the right to information. Unfortunately, the draft does not provide much guidance on the factors to be used to assess the situation or to help determine how the different interests should be balanced.

Under new Article 17a, "Right to Restriction of Processing", of the draft EU Data Protection Regulation the data subject would have the right to restrict the processing of personal data where:

- The accuracy of the data is contested by the data subject, for a period enabling the data controller to verify the accuracy of the data;
- The controller no longer needs the personal data for the purposes of the processing, but the data are

required by the data subject for the establishment, exercise, or defense of legal claims; or

- The data subject has objected to the processing pending the verification of whether the legitimate grounds of the data controller override those of the data subject.

The new Article 17b, "Notification Obligation Regarding Rectification, Erasure, or Restriction", of the draft EU Data Protection Regulation would require the data controller to communicate any rectification, erasure, or restriction of processing carried out to each recipient to whom the data have been disclosed, unless this proves impossible or involves a disproportionate effort.

The proposed language continues to be criticized by corporations as well as by some of the Member States themselves, for a variety of reasons. It is unclear at this point whether and how the provisions regarding the proposed "Right to be Forgotten and Right of Erasure" will be further modified.

If the concept is maintained in the final approved version of the EU Data Protection Regulation, its implementation is likely to cause much headache and frustrations because – at least in their current form – the relevant provisions are much too vague and provide little or no practical guidance. Guidelines published by the Article 29 Working Party (discussed below in this article) might go some way to provide the needed clarity and direction.

California Right of Erasure

In the United States, where the right of information and freedom of expression are strongly defended and enforced, the topic has been approached differently and in a narrower manner. Consistent with its sectoral approach, the United States has adopted laws governing specific sectors, such as the Fair Credit Reporting Act, discussed above in this article, which applies to the compilation and distribution of consumer reports and are still in effect.

Until recently however, there was no specific law to address the erasure or blocking of material previously posted on,

or available from, an online service. In the Fall of 2013, the California legislature passed the "Privacy Rights for California Minors in the Digital World Act." This law was the first of its kind in the country. It came into effect in California as of January 1, 2015.

The Law

The Privacy Rights for California Minors in the Digital World Act, codified as California Business & Professions Code § 22581[15], creates a right of erasure that has numerous similarities with the "Right to be Forgotten or Right of Erasure" included in the most recent draft of the proposed EU Data Protection Regulation. The California law requires an operator of an Internet Web site, an online service, or an online or mobile application (Web service) who has actual knowledge that minors are using its service to permit a minor who is a registered user of that Web service to request and obtain the removal of content or information posted on the Web service by that minor.

The Web service must inform its users of this right to remove or obtain the removal of content or information. It must, in addition, provide clear instructions on how a user may remove, or request and obtain the removal of, such content or information.

The law is very limited. It only applies to content or information that the user himself has posted on the Web service. It does not address content or information that was posted by a third party. Only content posted by a specific user can be removed at the request of that user.

The law provides for several exceptions to this "Right of Erasure." They include, among others, when the content has been made anonymous, when the minor has received compensation or consideration for providing the content, or when applicable law requires the Web service to maintain the content or information.

---

[15] Available at *http://www.leginfo.ca.gov/cgi-bin/displaycode?section=bpc&group=22001-23000&file=22580-22582*.

A Web service is deemed compliant with the law if it renders the content or information no longer visible to other users, even if the content or information remains on the Web service's servers in some form.

The Deficiencies

The Privacy Rights for California Minors in the Digital World Act is very narrow. The law applies only to Web services that are directed to minors or those that have actual knowledge that a minor is using the Web service. It only provides for the removal or blocking of content about an individual that was posted by that individual.

The California law does not address the issue of content about an individual that was posted by a third party. Unfortunately, content posted by a third party might be significantly more damaging than content posted by an individual. This would be the case, for example, of pictures posted by a third party attending or participating in the same event. These pictures could show a group of teenagers engaging in partying and drinking. Examples abound. The California law would not allow the removal of the group picture, except at the request of the person who held the camera.

The California Right of Erasure law also fails to address the growing concern about "revenge porn." There are increasing reports of publication on social media of pictures or videos taken in the course of a personal relationship. In these cases, upon the termination of a relationship, a disgruntled party publishes at-large embarrassing or revealing pictures of the other party. The California law would be unable to address these more egregious behaviors, in these cases, as well.

III. Decision of the Court of Justice of the European Union

In addition to the new legislative trends toward the recognition of a right to removal of certain information, the courts, worldwide, are beginning to become more receptive to the plea of individuals for the de-listing of search results that damage their

reputation when these search results reveal information that is obsolete or no longer relevant. Throughout 2014, several court decisions granted individuals a "Right to be Forgotten." The most significant of these cases was filed in Spain against Google Inc. (USA) and Google Spain. The case made its way up the different levels of the judicial system and ultimately reached the Court of Justice of the European Union.

Background

In May 2014, in a case against Google initiated by a Spanish man (*Costeja v. Google* case), the CJEU held that a European citizen has the right, under certain conditions, to demand that a search engine remove links to information pertaining to him that is "inaccurate, inadequate, irrelevant or excessive," even if the information is truthful.[16] The court found that the interference with Mr. Costeja's right to data protection could not be justified merely by Google Inc.'s economic interest.

In the *Costeja* case, the plaintiff was able to prevail because the CJEU found that Google Inc., a US based company, was subject to EU law as a data controller and that EU law required the removal of links to certain articles that had become "inaccurate, inadequate, irrelevant or excessive." This is an important decision because, until this juncture, plaintiffs had faced significant hurdles in their actions against Google Inc. and its subsidiaries. Prior cases had held that Google was not a data controller, and that Google Inc., which is responsible for the processing, was not subject to the jurisdiction of the local laws.

The judgment has attracted significant international attention, and some of the more controversial aspects of it have been subject to much critical opprobrium. However, it is worth remembering that many other aspects of the CJEU ruling are in keeping with developments that are already well underway at the European level. Viewed through this prism, one could argue that many of the less controversial elements of the *Costeja* judgment are merely natural precursors to, or an affirmation of, the "Right to

[16] CJEU Judgment available at *http://curia.europa.eu/juris/liste.jsf?num=C-131/12*

be Forgotten and to Erasure" provisions in the proposed EU General Data Protection Regulation. In addition, the *Costeja,* in its effect, is consistent with the provisions of the Fair Credit Reporting Act that prohibit the inclusion in credit reports of information that is older, depending on the nature of the information concerned, than 7 or 10 years old.

Territorial Reach of EU Data Protection Laws

The CJEU found that it had jurisdiction over Google Inc. even thought it is a US based company. The rules that define jurisdiction are very complex. In most cases, courts only have jurisdiction over persons located within their territory. In the *Costeja v. Google* case, Google Inc. argued that it was not subject to EU laws because all processing was conducted in the United States, and that its Spanish subsidiary was only intended to promote and sell products. However, the CJEU found that Google Inc. has an establishment in Spain through its subsidiary and that the processing is conducted in the context of the activities of that establishment. According to the CJEU, even if the physical server used to process EU residents' data is located outside the European Economic Area, EU laws apply to the foreign entity responsible for that server if it has a branch or subsidiary in a Member State and that branch or subsidiary promotes the sale of advertising space offered by the foreign entity.

US companies have often argued that they were not subject to EU laws because they did not operate directly on EU territory. The CJEU ruling significantly increases the probability that a foreign company operating in the EU through a domestic subsidiary might find itself subject to EU jurisdiction. A complex corporate structure with layers of subsidiaries might no longer successfully act as a shield from the application of EU laws. Under the CJEU decision, the presence of a subsidiary in a EU country, and a commercial link between the EU subsidiary and the US parent was deemed sufficient.

Search Engine as Data Controller

Google had argued, in the *Costeja case,* that it was only a data processor. However, the CJEU also found that a search engine is a data controller and not solely a data processor. The CJEU

stated that the "activity of a search engine consisting in finding information published or placed on the Internet by third parties, indexing it automatically, storing it temporarily, and making it available to Internet users according to a particular order of preference must be classified as 'processing of personal data' within the meaning of Article 2(b) [of the 1995 EU Data Protection Directive] when that information contains personal data and, the operator of the search engine must be regarded as the 'controller' in respect of that processing".

Again, the position adopted by the CJEU is consistent with the current trend in the European Union. Increasingly, EU agencies, data protection authorities, and the Article 29 Working Party are defining a sliding scale. Under this scale, the same company can be both a data controller for certain activities and a data processor for others. Two companies may be deemed joint data controllers. See, for instance, the A29 Opinion WP196, which points out that, in some circumstances, cloud service providers are acting as data controllers.[17]

US companies, including cloud service providers, have vehemently argued that they are solely data processors, and not data controllers. The *Costeja* ruling weakens their position with respect to this argument.

Data Subject's Right to the De-listing of Information

With respect to the de-listing request, the CJEU found that, under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union[18] as implemented, inter alia, by Articles 6, 7, 12, 14 and 28 of Directive 95/46/ EC of the European Union,[19] a data

---

[17] Article 29 Working Party, Opinion 05/2012, WP196, Section 4.1, available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf*.

[18] Charter of Fundamental Rights of the European Union, 2000/C 364/01, available at *http://www.europarl.europa.eu/charter/pdf/text_en.pdf*.

[19] European Union Data Protection Directive, Directive 95/46/EC of October 24, 1995, available at

subject may request that information about him no longer be made available to the public in a list of results. In most cases, these rights override both the economic interest of the operator of the search engine and the interest of the public in having access to that information upon a search relating to the data subject's name.[20]

However, if it appeared that the interference with his fundamental rights is justified by the preponderant interest of the general public in having access to the information from such a search, such as due the role played by the data subject in public life, then the request should be rejected.

When analyzing the rights of the data subject, the CJEU first pointed out that the provisions of Directive 95/46 must be interpreted in the light of fundamental rights that are set out in the Charter of Fundamental Rights of the European Union with respect to the processing of personal data that may infringe fundamental freedoms, such as the right to privacy.[21]

Article 7 of the Charter guarantees the right to respect for private life, and Article 8 of the Charter proclaims the right to the protection of personal data. Article 8(2) and (3) specify that such data must be processed fairly, for specified purposes, and based on the consent of the person concerned or some other legitimate basis laid down by law. These requirements are implemented inter alia by Articles 6, 7, 12, 14 and 28 of Directive 95/46.

The CJEU first noted that Article 7(f) of Directive 95/46/EC permits the processing of personal data where it is necessary for the legitimate interests pursued by the data controller or by third parties, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject — in particular his right to privacy with respect to the processing of personal data — which are protected under Article 1(1) of the Directive. Application of Article 7(f) of the Directive necessitates

---

http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

[20] Full text of the CJEU decision available at: *http://curia.europa.eu/juris/liste.jsf?num=C-131/12*

[21] CJEU Decision, § 68.

a balancing of the opposing rights and interests concerned, in the context of the data subject's rights arising from Articles 7 and 8 of the Charter. [22] The Court also noted that while the question of whether the processing complies with Articles 6 and 7(f) of Directive 95/46 may be determined in the context of a request as provided for in Article 12(b) of the Directive, the data subject may, in addition, rely on the right to object laid down in subparagraph (a) of the first paragraph of Article 14 of the Directive.

Subparagraph (a) of the first paragraph of Article 14 of the Directive requires Member States to grant the data subject, in certain cases,[23] the right to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, unless otherwise provided by national legislation. Such balancing enables the evaluation of the circumstances surrounding the data subject's particular situation. Where there is a justified objection, the processing instigated by the data controller may no longer involve those data.

The CJEU also noted that personal data processing carried out by a search engine operator may significantly affect an individual's fundamental rights to privacy and personal data protection when the search by means of that engine is carried out based on the individual's name. Indeed, the list of results enables any Internet user to obtain a structured overview of the information relating to that individual that can be found on the Internet. The compilation may concern a vast number of different aspects of the individual's private life, and it allows for the creation of a detailed profile of that individual. This information could not have been interconnected or the compilation obtained in such an easy manner without the use of a search engine.[24]

In the light of the potential seriousness of that interference, the CJEU found that "it is clear that it cannot be justified by merely the economic interest that the operator of such an engine has in that processing." However, to the extent that, in certain

---

[22] CJEU Decision, § 74.
[23] These exceptions are found in Article 7(e) and (f) of the Directive.
[24] CJEU Decision, § 80.

situations, the removal of links from the list of results could have effects on the legitimate interest of Internet users potentially interested in having access to that information, "a fair balance should be sought in particular between that interest and the data subject's fundamental rights under Articles 7 and 8 of the Charter."

While the data subject's rights generally override the interest of Internet users, this balance may depend on the nature of the information in question and its sensitivity for the data subject's private life and on the interest of the public in having that information. This interest may vary, in particular, according to the role played by the data subject in public life.

The Court concluded that Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 are to be interpreted as meaning that, in order to comply with the rights laid down in those provisions, a search engine operator is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages published by third parties and containing information relating to that person.[25]

In practice, according to the CJEU ruling: when appraising requests to oppose processing, it should be examined whether the data subject has a right that the information relating to him personally should no longer be linked to his name in a list of results displayed following a search made on the basis of his name.[26]

Under the CJEU decision, when evaluating the conditions for the application of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, it should be examined whether the data subject has a right that the information relating to him personally should no longer be linked to his name by a list of results displayed following a search made on the basis of his name, without it being necessary to find that the inclusion of the information in question in that list causes prejudice to the data subject. [27]

---

[25] CJEU Decision, § 88.
[26] CJEU Decision, § 96.
[27] CJEU Decision, § 97.

In most cases, the data subject's rights in this scenario override both the economic interest of the search engine operator, and the interest of the public in finding that information upon a search relating to the data subject's name. [28] However, that would not be the case if the interference with his fundamental rights were justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question. This would be the case, for example, if the data subject played a particular role in public life.

In the specific case at hand, the list of results that the Internet user obtains by making a search by means of Google Search on the basis of the data subject's name, provided links to a daily newspaper archives. These pages contained announcements mentioning the data subject's name and information about a real-estate auction connected with attachment proceedings for the recovery of social security debts. Based on the sensitivity for the data subject's private life regarding the information contained in those announcements and the fact that their initial publication had taken place 16 years earlier, the CJEU found the data subject had a right that the information no longer be linked to his name by means of such a list. Thus, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, the data subject may require those links to be removed from the list of results.

IV. Global Developments

In theory, the geographic scope of the application of the CJEU decision is limited to the EU territory. The EU data protection authorities have indicated that they will focus on claims where there is a clear link between the data subject and the EU, such as where the data subject is a citizen or resident of a EU Member State.[29]

---

[28] CJEU Decision, § 98.

[29] Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and

Nevertheless, the CJEU ruling has been followed with great interest throughout the world, and similar cases are being filed and adjudicated on outside of the European Economic Area. The ruling has clearly influenced judges and data protection authorities worldwide. The primary target of these cases has been Google Inc. due to the popularity and widespread use of its search engine. However, other search engines, as well as a wide range of corporate organizations have also received de-listing requests.

Japan

Japan has dealt with several cases in which individuals sued search engines in order to obtain the removal of certain links, pertaining to them, from search listings.

In October 2014, the Tokyo District Court issued an injunction ordering Google to remove search results that were hinting at past criminal activity of the plaintiff.[30] The plaintiff claimed that his privacy rights were violated due to these articles. The order required the removal of approximately 120 of the 230 search results identified. The court did not address the veracity of these articles.

Prior to this case, in January 2014, the Tokyo High Court had ruled in Google's favor in a case where a man was seeking an injunction involving the Google autosuggest function because when his name was typed in for a search it automatically would show words that falsely suggested criminal activity. The judge stated that damage suffered from such searches did not outweigh the damage that Google and other Internet users would suffer because of losing use of the autocomplete function. An appeal to

---

Mario Costeja Gonzalez" C-132/12, WP 225, available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.*

[30] *See*, *e.g.*, *Wall Street Journal*, October 22, 2014, "Google Japan Raises Issues of Right to be Forgotten," *http://www.wsj.com/articles/google-japan-case-raises-privacy-issues-1413981229*.

the Japan Supreme Court is pending.

Mexico

In January 2015, the Mexican Data Protection Authority ruled against Google on facts similar to those in the *Costeja* case. It found that Google Mexico is a data controller, and that it had to remove the offending information.

Argentina

In Argentina, there was an administrative decision, by the Data Protection Authority, against Google ordering the deletion of links because the information was outdated and it affected the honor of the individual concerned.

Australia

The Australian Privacy Commissioner has indicated that he is monitoring the developments in the EU, and how the industry and regulators are responding to the ruling globally.

South Korea

The South Korean Communication Commission has established a task force to look into possible legislation in order to make it easier for South Koreans to get their personal information removed from the Internet.

Hong Kong

In June 2014, the Privacy Commissioner stated that he is exploring the implication of the *Costeja* ruling, including the rights of users in the Asia Pacific region.

V. Article 29 Working Party's Guidelines

In late November 2014, the Article 29 Working Party (A29) published Guidelines in its Working Paper WP225 to clarify the position of the EU Data Protection Authorities on the issue of

the *Costeja* judgment. [31]

The A29 Guidelines address the practical implementation of the CJEU ruling and increase its scope. They opine that when a search engine implements a request under the "Right to be Forgotten," the de-listing should occur on all of its domains, and not just its EU based domains. Further, they clarify that while the CJEU ruling pertains to a search engine, it might apply to other intermediaries. These two aspects are especially relevant to US companies, which might find themselves caught unexpectedly in a "Right to be Forgotten" delisting request.

Not Just for Search Engines

The Guidelines expand the CJEU ruling to organizations other than search engines. The A29 advises that while the ruling is specifically addressed to generalist search engines, it does not mean that it cannot be applied to other intermediaries. The de-listing right may be exercised whenever the conditions established in the ruling are met.

It is not clear, at present, which types of organizations might be affected. The Guidelines do not identify these "other intermediaries." Potential targets might include entities that use or develop big data techniques, data brokers, credits reporting organizations, and other companies specializing in background checks, archives, library, or research organizations that offer searchable databases. Anyone who processes data that affect an individual may become a target.

---

[31] Article 29 Working Party, Guidelines on the Implementation of the Court of Justice of the European Judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-132/12, WP 225, available at *http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf.*

Territorial Scope of De-Listing

The A29 also believes that limiting de-listing to EU domains would not satisfactorily guarantee the data subjects' rights. De-listing decisions must be implemented in such a way that they "guarantee the effective and complete protection of data subjects' rights, and that EU Law cannot be circumvented." Thus, companies should expect that they might be required to implement de-listing requests on all relevant domains that they use or operate.

At a minimum, this worldwide implementation would result in significant increase in technical work and related administrative costs. In addition, there might be a conflict between EU and foreign laws and cultures. For example, the right of information and the freedom of expression are areas where EU and US laws differ. The First Amendment to the US Constitution has been interpreted broadly to protect the freedom of speech. European laws, on the other hand, may be narrower. For example, European law may restrict certain forms of expression that would be legal in the United States, such as hate speech. If publication of certain content might violate EU laws, the de-listing of the same content might violate some aspects of US law.

American companies with operations in Europe that might be subject to "Right to be Forgotten" requests may struggle to accommodate both viewpoints. At a minimum, they should be aware that a de-listing request might have to be implemented on all of their domains rather than just in a specific region. Whether and how they will be able to accommodate the nuances of US and EU freedom of expression laws remains to be seen.

Thirteen Criteria for Evaluation of De-Listing Requests

The second part of the A29 Guidelines contains the list of 13 "common criteria" that the Data Protection Authorities have agreed to apply when handling the complaints filed with their national offices following de-listing refusals. The A29 has advised that these criteria should be applied on a case-by-case basis and in accordance with the relevant national legislation. These Guidelines may become a valuable tool for companies, courts and data protection authorities that will be vested with the responsibility to receive, and rule on, de-listing requests.

According to the Guidelines, this list of criteria is to be seen as a flexible working tool to help Data Protection Authorities in their analysis of "Right to be Forgotten" complaints, and during their decision making process. No single criterion should be determinative. Each of the criteria has to be read in the light of the principles established by the CJEU and in particular in the light of the public's interest in having access to the information. The specific criteria are:

1. Does the search result relate to a natural person, *i.e.*, an individual? Does the search result come up against a search on the data subject's name?
2. Does the data subject play a role in public life? Is the data subject a public figure?
3. Is the data subject a minor?
4. Is the data accurate?
5. Is the data relevant and not excessive?
    a. Does the data relate to the working life of the data subject?
    b. Does the search result link to information that allegedly constitutes hate speech/slander/libel or similar offenses in the area of expression against the complainant?
    c. Is it clear that the data reflects an individual's personal opinion or does it appear to be verified fact?
6. Is the information sensitive within the meaning of Article 8 of the Directive 95/46/EC?
7. Is the data up to date? Is the data being made available for longer than is necessary for the processing?
8. Is the data processing causing prejudice to the data subject? Does the data have a disproportionately negative privacy impact on the data subject?
9. Does the search result link to information that puts the data subject at risk?
10. In what context was the information published?
    a. Was the content voluntarily made public by the data subject?
    b. Was the content intended to be made public? Could the data subject reasonably have known that

the content would be made public?

11. Was the original content published in the context of journalistic purposes?
12. Does the publisher of the data have a legal power or a legal obligation to make the personal data publicly available?
13. Does the data relate to a criminal offense?

VI. Freedom of Speech and Right of Information versus Right to Be Forgotten

The different facets of the "Right to be Forgotten or Right of Erasure" raise many complex issues. It is clear that much iteration will be needed before a reasonable and practicable solution may be reached, if any. While the A29 Guidelines help narrow the issues and identify methods for balancing the different interest, they address only one part of the issue, its practical implementation.

There are numerous other critical issues to be addressed. The most critical of these surrounding issues is the effect on freedom of speech, and right to information. The CJEU ruling, the A29 Guidelines, as well as the different versions of Article 17 of the EU General Data Protection Regulation, stress that the "Right to be Forgotten" must be balanced against other fundamental rights, such as the freedom of expression and the freedom of the media. How can this be done? Who would have enough knowledge and experience to make the decision? How can we be assured that enough precedents and criteria are created? How can we ensure that the evaluation and balancing process is conducted in such a way that the process is repeatable, and that similar fact patterns are decided in a similar manner?

The matter becomes even more complex in the global setting, as different countries may have different views and different legal frameworks with respect to freedom of speech or freedom of information. The concepts themselves may be different. The applicable laws, if any, may be overridden by other laws or may have exceptions unique to a particular country.

The position taken by the A29 Guidelines that a de-listing decision should be implemented worldwide on all domains of the organization that receives the delisting request may be difficult to implement. It is not clear on which grounds a de-listing decision made in a particular country or region would be enforceable in a different jurisdiction. In addition, assuming that this might be enforceable, implementation might be unworkable due to conflicts with local laws.

The CJEU decision refers to the removal of information that has become "inaccurate, inadequate, irrelevant or excessive" for the purpose for which it was processed. In those situations where one tries to erase information about criminal conviction or similar events, who is to judge that the particular information is "inaccurate, inadequate, irrelevant or excessive?" There may be cases where existing laws have already addressed a similar issue and might provide guidance. For example, in the United States, under the Fair Credit Reporting Act, information about personal bankruptcy must be removed from a credit report after a certain period has elapsed. This tangible metric might be useful in a context similar to the *Costeja* case. However, these metrics are likely to be different from one country to another, even within the European Union itself.

Further, according to the reasoning of the CJEU and that of the A29, an assessment must be conducted on a case-by-case basis. Different elements must be examined, such as the type of information in question or its sensitivity for the individuals' private life. The role that the person requesting the de-listing plays in public life and the public's interest in having access to the information must be evaluated, as well. It seems unwise and unreasonable to expect that a search engine would be qualified to make the evaluation. Giving search engines the power to examine and rule on de-listing requests seems the wrong strategy. They are not equipped to make this type of assessment.

There are significant ethical and societal implications in removing or not referencing information that can be unearthed only because of the extraordinary power of search technologies. Search engines may not be the best judges to decide whether and what information should be available to society. The United

Kingdom and the United States are questioning the soundness of giving search engines this power.

In other circumstances, trained judges, arbitrators or mediators, rather than private companies, have been entrusted to evaluate the merits of claims made by an aggravated party. It would make sense if search engines, data brokers, and others were relieved from this responsibility, and governments or data protection authorities found a more objective and efficient way to evaluate and implement "Right to be Forgotten" requests. For example, trained ombudsmen could be appointed to review, directly, all requests from an individual regarding a particular article. The ombudsman's decision would bind all search engines.

VII. A Right to Obscurity?

Many individuals hope to be able to erase or mask a portion of their past—a mistake, a petty crime for which they have paid, events that occurred in a distant past, or simply articles about them that they find invasive—such as news regarding their health. The CJEU ruling, the A29 Guidelines, and the recent series of "Right to be Forgotten" cases give them an opportunity to request such masking and in some cases, to obtain it.

In March 2015, FTC Commissioner Julie Brill commented that the CJEU decision in the *Costeja v. Google* case was not as incompatible with U.S. laws or ideals of free speech as some critics of the decision have suggested.[32] She noted that the CJEU decision would be better classified as allowing a "right to obscurity." She also observed that an improved "right to obscurity" would be particularly valuable in regard to information held by data brokers that is used for "people search" services, such as a requirement for data brokers to allow people to see information in their data files, and either correct or expunge it, if warranted.[33]

It is clear that the "Right to be Forgotten" or "Right of

[32] Wilson, "*FTC's Brill Backs Enhanced Consumer "Right to Obscurity*", Law 360, March 10, 2015.
[33] Id.

Erasure" or "Right to Obscurity" is still in its infancy. It needs to be refined and to become more nuanced in order to provide workable guidelines and a truly balanced approach. In the meantime, more complex issues will continue to arise and will, undoubtedly, force more in-depth analysis. It is also clear that requests for the removal or blocking of information or search results will not disappear in the near future. The concepts will evolve and be refined as more cases of this nature are evaluated by learned judges. The recent events have raised great interest and much comment throughout the world.[34] It is clearly a global phenomenon that would gain from being studied at the global level.

Countries cannot keep ignoring the ubiquity of the Internet, social media, and other communication means. US companies, including search engines, data brokers, credit reporting agencies, and other organizations that offer search capabilities or operate databases should stay tuned and understand the likely implications of the recent cases, guidance and laws on this issue.

[34] *See*, *e.g.*, *Wall Street Journal*, October 22, 2014, "Google Japan Raises Issues of Right to be Forgotten," *http://www.wsj.com/articles/google-japan-case-raises-privacy-issues-1413981229*.