April 2016

The Right To Be Forgotten

Lisa Owings

Please take a moment to share how this work helps you through this survey. Your feedback will be important as we plan further development of our repository.

Follow this and additional works at: http://ideaexchange.uakron.edu/akronintellectualproperty

Part of the Intellectual Property Law Commons

Recommended Citation


This Comments is brought to you for free and open access by Akron Law Journals at IdeaExchange@UAkron, the institutional repository of The University of Akron in Akron, Ohio, USA. It has been accepted for inclusion in Akron Intellectual Property Journal by an authorized administrator of IdeaExchange@UAkron. For more information, please contact mjon@uakron.edu, uapress@uakron.edu.
THE RIGHT TO BE FORGOTTEN

Lisa Owings*

I. INTRODUCTION

In the early days of the Internet, people were concerned with the technical details of sharing information. Now, people are concerned with how to remove information and what rules should govern information removal. Currently, few legal protections guarantee persons the right to

1

Owings: The Right To Be Forgotten
remove negative data about themselves from the Internet.¹ In the United
States, these rights are practically non-existent. The right to remove
negative data could include medical data, past foreclosures, or unwisely
posted photographs. Although it may be technically impossible to
destroy the data, certain processes can make the information difficult for
people to find—essentially forgetting that it exists.

In Spain, the courts elevated the ability of Spanish citizens to
remove irrelevant and outdated information to that of a right.² Irrelevant
and untimely information is essentially information that is not relevant
to the circumstances for which it is sought or information that is no
longer true. Following the provisions of the European Union (EU)
Directive on Data Protection,³ the court said that a person has a
“fundamental right” to privacy that extends to the removal of
information about the individual.⁴ Because of the decision, Google now
offers European users the ability to remove data via an online form.⁵
Nevertheless, this form is untested in the sense that it is unclear what
standards Google applies to determine whether the information is
irrelevant or untimely. Google claims its practices balance privacy rights
of the individual with the public’s right to know and distribute the
information.⁶ This is essentially a balance between privacy and free
speech; however, Google does not state the factors it will use to make its
determination. Furthermore, Google maintains that it may decline to
remove information that is in the public interest, such as information
about public officials.⁷ Additionally, pending legislation in the European
Union could affect Google’s ability to use its form based on the final
language at the time of passage.⁸

¹ Lisa Owings received her J.D. and LL.M. in Intellectual Property from The University of Akron
School of Law. She would like to thank her family, Seamus and Aine.

² Sarah A. Downey, How to Delete Things From the Internet: A Guide to Doing the

³ See generally Case-131/12, Google Spain SL v Agencia Española de Protección de Datos
SL].


⁶ Id.

⁷ Id.

⁸ EUROPEAN COMMISSION, FACTSHEET ON THE “RIGHT TO BE FORGOTTEN” RULING
Many in the United States are closely watching the impact of the Spanish Google case and the EU’s proposed legislation because it will affect large American corporations. The Spanish case involved Google search results, and other internet sites based in the United States are trying to navigate what the law and ruling could mean for them. Many corporations, such as Google, are concerned because their business consists of selling information or targeted ads constructed from a user’s information. If users are able to remove information about themselves through data privacy laws, then sites based on the selling of personal information have less information and incomplete packets of information to sell, which will almost certainly cause a drop in profits for such sites. There is concern in the United States about the right to be forgotten because U.S. citizens lack the same data privacy protections that European citizens have, as demonstrated by the Spanish Google case. European citizens may be concerned about the right to be forgotten because they are unclear about the pending changes to the law and their legal protections. Worldwide, individuals might be concerned that blocking information for some people and making it available to others creates an information oligarchy and an inconsistent Internet.

This Article advocates a new test for balancing free speech and privacy interests online. There should be a three-prong test for whether, and under what circumstances, a user may request deletion of online data under the right to be forgotten. First, if the information is the publication of a private fact that is offensive to a reasonable person and not newsworthy, it should never be published unless the individual chooses to do so. Second, if individuals posted the information about themselves or as an expression of their opinion, they should have the right to remove it. This should apply not only to sensitive information such as financial or medical data, but to any data the individual posts. Third, if the information is not relevant to the circumstances under which it has been posted or is outdated, and if there is not a compelling reason for it to remain publicly available, then it should be removed. These prongs may stand alone or overlap depending on the circumstances of the individual. Current legal protections, especially in the United States, are scarce and lack effective means of enforcing the removal.

Part Two of this Article focuses on the Spanish court ruling and its

---


impact on Google. The section will discuss what the court means when it says the information should be relevant and timely and why these are necessary for information removal. Part Two also discusses how Google began implementing the ruling and why this may not be the best solution for allowing individuals to remove results from Google’s site. Finally, Part Two discusses counter-arguments to the ruling and the merits of each.

Part Three discusses the proposed European Union data law, which recognizes a right for individuals to have data privacy in their online interactions. It discusses the history and current status of the proposal, and the arguments against its passage. Part Three also focuses on how such a law would be implemented and potential negative effects that could result from the law.

Part Four promotes a global solution that recognizes and respects the Google ruling and the EU proposal, but also respects free speech. By passing a law in the United States that is substantially similar to the proposal in the European Union, the law would not only allow corporations to know where they stand but also prevent a “patchwork Internet” that would result from some nations having access to search results that other nations do not. This patchwork Internet should be avoided except when the search engine is providing specifically local results because it impairs the consistency of information that is available throughout the world. Although the United States is under no obligation to pass or follow a European law, many of the corporations at the center of the right to be forgotten controversy are U.S. corporations. By passing a data removal law, the United States would be able to apply its own goals for information privacy and determine what online privacy it will allow its citizens to protect.

By enacting laws throughout the major nations of the world and applying the suggested three-prong test in constructing those laws, people from remote locations can access the same information throughout the world. For example, a uniform law would allow a user who lives in London to access the same search results when he is visiting the United States as he expects at home. This is important to preserving the consistency of information across the global online marketplace. The proposed three-prong test serves the purpose of guiding nations as they construct laws to determine quickly how to handle data privacy concerns.
II. GOOGLE SPAIN V. GONZALEZ AND THE EFFECT OF GOOGLE

A. Background and Procedural History of the Case

On January 19, 1998, a Spanish newspaper called La Vanguardia published a regular edition of their newspaper. On page 23 was an auction listing from the Labour Ministry that listed all property seized by the Social Security Department for attachment proceedings to recover social security debt. Among the seventeen listed properties was a small property in Catalonia, Spain. Before the auction, Mario Costeja González and his wife owned this property. The foreclosure amount appears to have been for less than $55,000 at the time of the listing.

In 2009, the newspaper began publishing all of its past and present newspapers online. This allowed users to search La Vanguardia as far back as 1881 at no cost. By then, Mr. González was divorced, and his debt was discharged. He presumably performed an “ego search” on Google, which is when a user searches the Internet for his own name to see what information is available. When he entered his name, one of the first results was page 23 of La Vanguardia’s newspaper showing the property auction. González contacted La Vanguardia to request removal of the information under Spanish law. La Vanguardia claimed it published the information lawfully under the direction of a State agency. González then tried to remove the information from Google search results.

Google indexes websites by following links from page to page. Google then applies its confidential algorithm, which Google claims

12. Id.
13. Id.
14. Id.
16. derechoaleer, supra note 11.
17. Id.
18. Id.
19. Id.
20. Id.
21. Id.
22. Id.
23. Id.
uses over 200 factors to determine how to rank search results. Google also claims to fight spam in its search results so that it may keep the results relevant.

It is on this latter claim that González focused his argument. He said that when one of the first search results to appear when a user enters his name is a foreclosure result from 10 years earlier, the information is neither relevant nor timely. When González sued, he wanted Google to remove or conceal the personal data so that the personal data would not be included in search results about him and would not appear in the links to La Vanguardia. In addition, González wanted La Vanguardia to remove or alter the pages so his personal data no longer appeared, or to use tools to prevent search engines from accessing the data because the information was no longer relevant.

Procedurally, under EU law, González sought a decision from the Agencia Española de Protección de Datos (AEPD) on the removal of the information from both the newspaper’s records and Google’s search records. On July 30, 2010, the AEPD rejected the claim against La Vanguardia because the AEPD found the newspaper was legally justified to publish the information about the attachment proceedings. The publication wanted to bring as many people as possible to the auction. In contrast to finding justification for the newspaper, the court upheld the complaint against Google. The AEPD said that search engines are subject to data protection laws since search engines carry out data processing functions and act “as intermediaries in the information society.” The AEPD recognized that it might not be necessary to remove the data from the websites where the information originally appears, but Google may still have a duty to the data subject to remove it. In other words, La Vanguardia published it properly because the information was timely when published and was relevant because the publication intended to attract people to the auction. However, Google’s publication was not timely or relevant. It was not timely because Google

29. Id. ¶ 16.
30. Id. ¶ 17.
31. Id.
32. Id. ¶ 22.
linked to it 10 years after the auction took place, and it was irrelevant because Google did not intend to bring people to the auction when it published the search results.\textsuperscript{33}

Google brought a separate action against the decision to the Audiencia Nacional, which is Spain’s highest court.\textsuperscript{34} The court joined the actions.\textsuperscript{35} The Audiencia Nacional said there is a question of what obligations

are owed by search engines to protect personal data of persons concerned who do not wish that certain information, which is published on third parties’ websites and contains personal data relating to them that enable that information to be linked to them, be located, indexed and made available to internet users indefinitely.\textsuperscript{36}

The court referred that question to the Court of Justice of the European Union (CJEU). The CJEU applied Directive 95/46\textsuperscript{37} of the European Parliament and of the Council of October 24, 1995, which discussed the “protection of individuals with regard to the processing of personal data.” Article 1 of Directive 95/46 states that in order to give individuals protection, “any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States.”\textsuperscript{38} In this case, the member state was Spain, so Spanish law applied.

\section*{B. Does Google Process Data?}

The court first considered whether Google processes personal data under Article 2(b) of Directive 95/46. The court framed this in terms of a third party placing information on the Internet, Google indexing it automatically, Google storing it temporarily, and then Google applying its own algorithms to determine where the information should appear in a list of links, i.e. the search results. If Google processed personal data, does that make Google a “controller” under Article 2(b)?

Google claimed it did not “process” information because its algorithms do not distinguish between personal data and other information on the page. For example, on the same page as the newspaper’s listing of González’s foreclosure was an article concerning a euthanasia debate in Parliament. Google claimed it did not distinguish

\begin{footnotesize}
\begin{itemize}
\item[33.] Id. ¶ 15.
\item[34.] Id. ¶ 18.
\item[35.] Id.
\item[36.] Id. ¶ 19.
\item[38.] Id.
\end{itemize}
\end{footnotesize}
between González’s name and the debate in Parliament. Google also argued that even if its activity is data processing, it does not mean a search engine is a controller regarding that knowledge because it has no knowledge of the data and does not control it.39

González argued the opposite. He claimed the activity was data processing under Directive 95/46 and there are differences between a search engine’s data processing and the data processing of websites that originally publish the information.40 He argued that a search engine has its own objectives in processing the data, which is distinct from the original publisher.41 Furthermore, he argued search engines were controllers since it is the operator that determines the “purposes and means of that processing.”42

The court looked at Article 2(b) of Directive 95/46, which defines processing of personal 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.43

The court cited prior case law that said loading personal data on an internet page is processing under Article 2(b).44

Because it was uncontested that Google found, indexed, stored, and made the data available to search engine users, and since the information included personally identifiable information, it was personal data.45 Because a search engine collected that data and made it available, it processed it under Article 2(b).46 The court held that it did not matter that the newspaper previously published the information and cited prior cases that found the failure to apply Article 2(b) to previously published information deprived “the directive of its effect.”47 The court pointed out that Article 2(b) does not require alteration of the information to apply the label of “processing of personal data.”48 Storage, retrieval, or

40. Id.
41. Id.
42. Id.
43. Id. ¶ 25.
44. Id.
45. Id. ¶ 27.
46. Id. ¶ 28.
47. Id. ¶ 29.
48. Id. ¶ 31.
collection is sufficient.

The court specifically noted that the "organisation [sic] and aggregation of information" done by a search engine may allow users to search based on an individual's name. This can allow someone to gather a detailed data profile of the individual simply by typing in his or her name. This is significant to the overall ruling because the court found the search engine significantly affected a person's right to privacy because of this aggregation: It collected this information, ranked it, and made a more complete data profile than a mere website.\(^5\) This is true. Someone who searched *La Vanguardia*’s website would certainly discover that on January 19, 1998, González was one of seventeen people listed on page 23 as having a foreclosure auction.\(^5\) However, when one types in González's name in a Google search, there is both more and less information available about him. There is more information in the sense that someone may be able to find, among other things, his phone number, address, where he worked, whether he was on Facebook, opinions he posted on various sites, and whether he had his own website. There is less information in the sense that one of the results was this foreclosure. While people could probably understand via a preview of the site that this was a foreclosure, they had no real context for the information. The entry would probably appear as if it was posted in 2008 when the newspaper posted previous editions of the newspaper online. Therefore, even the date of the information appeared incorrect on the search results.

This is why the court ruled that, since a search engine can so profoundly affect the personal data, the activity meets the requirements of Directive 95/46, and the directive requires that search engines process data under the Directive's requirements.\(^5\)

The court held that it does not matter whether a robot or crawler carried out this indexing, nor does it matter if websites fail to exclude themselves from automatic indexes via a "noindex" code that the search engine is not responsible for the data processing.\(^5\) Article 2(d) allows that a determination can be made "alone or jointly with others."\(^5\) In answering the first question, the court held that Google and other search

\[\text{References:}\]

49. *Id.* ¶ 37.
50. *Id.*
51. *Id.* ¶ 14.
52. *Id.* ¶ 38.
53. *Id.* ¶ 39.
54. *Id.* ¶ 40.
engines process personal data and are controllers under Article 2(d).55

C. Does the Directive Apply to a U.S. Corporation?

Next, the court turned to the jurisdictional question of whether Directive 95/46 could apply to Google since Google is a worldwide corporation based in the United States.56 The court noted that in many Member States, Google offers a local version that uses the national language.57 For example, in Spain, the website appeared under the internet address of www.google.es, and the search results often displayed in Spanish.58 Google registered this website on September 16, 2003.59 Google indexed websites throughout the world, including those in Spain.60 Google Search compiled the search results and made money by displaying advertisements alongside search results.61 Google has a Spanish subsidiary called Google Spain, located in Madrid, Spain.62 It focuses on securing advertisers in Spain and serves those ads on Spanish search results and websites.63 This presented a unique dilemma: Google was based in the United States but targeted its work for Spanish people by using very local practices.

The court considered whether Article 4(1)(a) of Directive 95/46 can be interpreted to mean that processing personal data is carried out by a controller under one of three circumstances: first, whether the operator of a search engine has a subsidiary that promotes advertising space by the engine and directs its activity towards that Member State; second, whether the parent company designates a subsidiary within the Member State for two filing systems that relate to data of the customers who have contracted for advertising; third, whether the subsidiary forwards requests and requirements by data subjects to a parent company outside the European Union.64

González argued that there was an unbreakable link between Google and Google Spain, and the processing of personal data is in context of that establishment.65 Google argued that Article 4(1)(a) did

55. Id. ¶ 41.
56. Id. ¶ 42.
57. Id. ¶ 43.
58. Id.
59. Id.
60. Id.
61. Id.
62. Id.
63. Id.
64. Id. ¶ 45.
65. Id. ¶ 47.
not apply in the first condition. The court held that in the preamble to Directive 95/46, "establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements," and the "legal form of such an establishment, whether simply [a] branch or subsidiary with a legal personality, is not the determining factor." Because Google Spain engaged in real activity through stable arrangements in Spain and was a subsidiary of Google on Spanish territory, it is an establishment under Article 4(1)(a).

This answers the question of how a European court can subject an American company to liability. If Google did not have a Spanish division of the company, it would be difficult for a European court to enforce a judgment against Google. However, the court held that, when Google made a profit by creating Google Spain and showing ads in Spanish to Spanish searchers, Google could expect to be subject to rulings in Spain because it was in the context of the activities of the establishment. This ruling is consistent with rulings in the United States that deal with minimum contacts of subsidiaries to foreign corporations. Thus, the court was not using any different criteria than an American court would have applied in finding that a company could be liable for the acts of their subsidiaries.

D. Must the Search Engine Remove Links to Results That Third Parties Lawfully Published?

Next, the court considered whether Article 12(b) and subparagraph (a) of Article 14 mean that in order to comply with the provision, the search engine must remove results containing a person's name when third parties publish websites containing the name. This removal is particularly relevant when the information on the websites was lawfully printed. In other words, because La Vanguardia published the notice of foreclosure lawfully and did not have to remove it, and Google did little beyond include that information in a list of links, how can the court ask Google to remove the link when the newspaper does not have to?

66. Id.
67. Id. ¶ 48.
68. Id.
69. Id. ¶ 49.
70. Id. ¶ 56.
72. Google Spain SL, supra note 2, ¶ 62.
Google argued that any request to remove the information should have been directed to the newspaper because it made the information public, the newspaper can determine the lawfulness of the publication, and only the newspaper has the “most effective and least restrictive means of making the information inaccessible.”\textsuperscript{73} Predictably, González argued that he is under no obligation to ask the newspaper to remove it first.\textsuperscript{74}

There was some debate on this particular question between the various governments submitting briefs to the González court. This debate highlights the difficulty in constructing a law that would apply throughout the world. Each nation has its own policies that it wishes to achieve, and each has a somewhat different means of trying to achieve those policies.

Austria argued that a national supervisory authority may only order an operator to remove information published by third parties if the data was previously found to be unlawful or incorrect, or if the data subject has made a successful objection to the publisher of the website where the information was published.\textsuperscript{75} This is an attractive argument. If the newspaper published unlawful or incorrect information, the newspaper should delete it. Furthermore, Austria did not see the harm in forcing the user to make a request to the website first before escalating his objection to Google as the controller.

The Spanish, Italian, and Polish governments agreed with González that there was no need to approach the original publishing website before the matter escalated to Google.\textsuperscript{76} This idea has some merit as well. Information on the Internet has become difficult to forget. People can start websites and forget about them, leaving enormous amounts of data available for public viewing long after the information is no longer relevant or timely. When a website is abandoned, there may be nobody answering emails to respond to a takedown request.\textsuperscript{77} Furthermore, if the information is correct when published, as it was in González, the data

\begin{itemize}
  \item \textsuperscript{73} Id. ¶ 63.
  \item \textsuperscript{74} Id. ¶ 65.
  \item \textsuperscript{75} Id. ¶ 64.
  \item \textsuperscript{76} Id. ¶ 65.
  \item \textsuperscript{77} For example, consider the situation where a mother creates a website to share family photographs and pictures of her child, beginning at birth. The mother would need to register the website, presumably with a valid email address, and create the framework for photo sharing. As the child grows older, the mother may decide to stop posting pictures to the website in lieu of other options, such as social media accounts (e.g., Facebook). Unless the mother scrapes the Internet to remove links to her website or physically removes her original website with family photos, those photographs could be available indefinitely. Even if someone were to email the account holder, the mother may no longer check that account, divert emails by filtering, or ignore emails with foreign email addresses.
\end{itemize}
subject may not have any remedy to require removal and would have to resort to requesting Google remove the information anyway.

The Polish government, although it agreed with González that the person could submit a request directly to Google, argued that when the newspaper publishes information lawfully, González would have no recourse in getting the information removed from Google. The lawfulness of the information on La Vanguardia is imputed to Google, and it may include a link to lawfully published information on third party websites. This too has some merit. If the information is lawfully published, Google will assume there is a compelling reason for that information to be publicly available. Otherwise, a law would have weeded out any information that should not have been published. So if the information was lawful and all Google did was index the information and provide it amongst other links, the information should not suddenly become verboten just because of Google’s actions, which are miniscule in comparison to the original publishing.

The court began its analysis of this question by recognizing that the Directive provides a “high level of protection” in privacy to the processing of personal data. The court describes a balancing act between those who are processing the data and those whose data are being processed. The data processors have the duty to preserve “data quality, technical security, notification to the supervisory authority and the circumstances under which processing can be carried out.” Data subjects have the right to “be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances.”

Article 7 of the EU Directive on Data Protection guarantees respect for private life, and Article 8 gives the right to protection of personal data. Article 8, sections (2) and (3), provide that data has to 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,” access to data that has been collected about them, and the right to have that data “rectified.”

Article 12(b) says that the Directive requires that Member States

---

78. Google Spain SL, supra note 2, ¶65.
79. Id. ¶66.
80. Id. ¶67.
81. Id.
83. Id.
84. Google Spain SL, supra note 2, ¶69.
85. Id.
guarantee every data subject can rectify, erase, or block the processing of data that does not comply with the Directive, “in particular because of the incomplete or inaccurate nature of the data.” Article 6 allows Member States to create provisions for historical, statistical, or scientific purposes, but the controller has the responsibility of ensuring the data are processed fairly and lawfully. The court specifically held that the information must be “collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes,” and “adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.” The information must be “accurate and, where necessary, kept up to date” and “kept in a form which permits identification of data subjects for no longer than is necessary for purposes for which the data were collected or for which they are further processed.”

Article 7 deals with processing such as a search engine would handle. It allows processing personal data when it is necessary to carry out legitimate interests pursued by the controller, except where those interests are “overridden by the interests or fundamental rights and freedoms of the data subject.” The court said the data subject’s right to privacy applies in particular here.

Since subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 allows a data subject the right to object at any time on “compelling legitimate grounds relating to his particular situation to the processing of data relating to him,” if the request is compelling and legitimate, the controller may no longer process the objectionable data.

The court held that the requests may go directly to the controller who examines the merits of the objection, and if it is compelling and legitimate under Article 12(b), the controller must remove the data. When the controller decides not to remove the data, the data subject can bring the matter to the supervisory authority of the member state. The reason Austria was incorrect is that the court notes the search engines are bringing together various aspects of a person’s life that were not previously linked and making them interconnected. The court said the

86. *Id.* ¶ 70.
87. *Id.* ¶ 72.
88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.* ¶ 73.
92. *Id.* ¶ 74.
93. *Id.* ¶ 76.
94. *Id.* ¶ 82.
"operator of a search engine is liable to affect significantly the fundamental rights to privacy and protection of personal data . . . since that processing enables any internet user to obtain through the list of results a structured overview of the information relating to that individual that can be found on the internet."\footnote{95} Because the search engine can so significantly influence the processing, it cannot be justified simply by "economic interest."\footnote{96}

The reason the Polish government was incorrect is similar. It assumed that if the information was relevant and timely when it was first published, that it remained relevant and timely when Google placed a link, but it ignored the processing that Google did. Gathering pieces of González’s life from webpages that were not otherwise connected to each other makes a data profile of González. By placing the results of the foreclosure on the first page of link results, Google was essentially saying that this was an important or relevant fact that a person should know about González. A user who was specifically searching for records of González’s home ownership history might want to know this information, but it is difficult to argue that someone simply typing his name should have access to this data and that it should be considered an important fact about him.

In essence, the ruling made Google responsible for Google’s actions and the newspaper responsible for its actions. In paragraph 86 of the opinion, the court stated: "publication of a piece of personal data on a website (does) not necessarily coincide with that which is applicable to the activity of search engines."\footnote{97} Further, "the legitimate interests justifying the processing may be different and . . . the consequences of the processing for the data subject, and in particular for his private life, are not necessarily the same."\footnote{98} The court recognized that Google has a different interest in publishing the links, and just because the newspaper published the information with a legitimately protected reason does not mean Google has the same purpose in publishing the link.\footnote{99}

E. **May González Force Removal of True But Prejudicial Information?**

The final question the court considered was whether Article 12(b) and subparagraph (a) enable the data subject to require a search engine
to remove links to a third party because the information may be prejudicial to him or he wants that information to be forgotten after a certain time. In this case, the third party was *La Vanguardia*. Google argued the links should remain because it has nothing to do with the Directive and there was not a compelling legitimate ground. Google further argued the Directive did not address processing information that may be prejudicial or that the data subject wants forgotten. González cited the fundamental right to privacy that the court previously mentioned and says this extends to the right to be forgotten. This right to be forgotten overrides any legitimate interest of the search engine operator and the general interest in the information.

The court went back to an earlier portion of the decision. The court reiterated that when publishing personal data, it has to be kept in mind that the Directive applies to incorrect or wrong data. Additionally, the Directive also applies to facts that are "inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical, or scientific purposes." Restated, data can expire. It does so when data is lawfully published but is no longer relevant or is inadequate under the circumstances. When that occurs, the data expires and the results must be erased.

The court held that these results should not be linked to González by name when someone searches for his name. Specifically, González's right to privacy trumps Google's economic concerns and the general right of the public to the information about González's foreclosure. However, the court did not extend this too far. It said that there may be instances where the public life of the individual creates a compelling reason why such results should be publicly available. This is a "public figure" recognition where the lives of public figures are under a higher-level of scrutiny than private individuals, and courts recognize that there may be legitimate reasons why general public knowledge

---

100. *Id.* ¶ 89.
101. *Id.* ¶ 14.
102. *Id.* ¶ 90.
103. *Id.*
104. *Id.* ¶ 91.
105. *Id.* ¶ 92.
106. *Id.* ¶ 93.
107. *Id.*
108. *Id.* ¶ 94.
109. *Id.* ¶ 96.
should trump an individual’s privacy.\textsuperscript{110}

Since that was not the case with González, the information should be removed. González is a private individual, and he has rights under the Directive that give him the right to have private details about him removed. Information that is lawfully published could not be removed; however Google, as a controller, is compelled to respect his removal request when he objected that it was no longer timely or relevant. González did not need to apply first to the website for removal of information but instead could object directly to Google. Since the information on Google was excessive in relation to the purposes of Google’s processing, it should be removed.

F. Google’s Efforts at Compliance and Potential Problems

To date, Google has placed a form on its website that allows a user to submit a request to remove the information.\textsuperscript{111} This form is difficult to find. The form cites the González case and says that in response to it, “certain people can ask search engines to remove specific results for queries that include their name, where the interests in those results appearing are outweighed by the person’s privacy rights.”\textsuperscript{112} Google states that it will balance those privacy rights with the public’s interest to know and the right to distribute information.\textsuperscript{113} Google will look at whether the information is outdated and whether there is a public interest in the information. Specifically, Google says it may “decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials.”\textsuperscript{114} In order to process the request, Google requires a person to supply identification.\textsuperscript{115}

There are currently a few problems with Google’s form. While it had over 12,000 requests on the first day,\textsuperscript{116} the form itself is untested in the courts. This is not necessarily a problem because it does not have to be litigated to comply. The problem is that there will be cases that do not meet Google’s standards for removal that should potentially be removed.

\textsuperscript{110} Id. ¶ 81.
\textsuperscript{111} Search Removal Request, supra note 5.
\textsuperscript{112} Id.
\textsuperscript{113} Id.
\textsuperscript{114} Id.
\textsuperscript{115} Id.
New questions will arise as other cases work their way through the courts. Though the form is new, Google will likely need to modify it to comply with other rulings that occur. For example, if someone requests removal of information concerning professional malpractice, the form says the information does not have to be removed. But there may be a valid reason, given the circumstances, for removing that particular information. The courts would certainly be able to address the information removal request, but the form is factually incorrect in stating that it would require the information to remain. It states that Google may refuse to remove information of that type. Other rulings may determine that a person is not required to provide identification. Again, the form would have to be updated to remove the portion of the form that asks a user to upload his identification documents.

In addition, a new data protection law has been proposed and heavily discussed throughout the European Union. If passed, Google may find new requirements it must meet that the current form does not address. One of the potential changes that would come from passage of the proposal would actually benefit Google. Under the González ruling, each Member State must set its own data protection laws to meet minimum standards. The proposal would apply to all countries in the EU to create uniformity. This significantly lessens the burden on Google because Google’s form currently asks which Member State’s law applies to the data subject. Currently, Google must be aware of and comply with the various laws of each Member State. Under the new proposal, only one law would apply as each member state ratifies the General Data Protection Regulation.

One unsolved question of the ruling is how to accomplish data removal. For example, González said that Google should not have linked his name to the foreclosure newspaper listing. The court found that the newspaper validly published it in connection with his name, but Google did not. So, the article becomes essentially invisible in the search results for González’s name. However, is Google on notice as far as the others listed in the same newspaper posting? Given that Google displays a small section of each page where the words appear so that a user can

118. Id.
120. Google Spain SL, supra note 2, ¶¶ 16-17.
see some of the context of the result, if González’s name appears on a different person’s search results, has Google gone too far? The courts must still answer these questions.

G. Early Effects of the Ruling

One site has already pointed out that Google has placed a warning at the bottom of every European version of the search engine when a search for a name is completed. The warning says, “Some results may have been removed under data protection law in Europe.” In testing this at Google Ireland’s search engine, it did indeed appear as though a request was made to remove information from the search results. On one hand, this is beneficial to privacy advocates. If the warning appears in connection with every name, it is impossible to tell exactly which users have requested removal of data. This is problematic in that it presents an incomplete or inaccurate picture of the data subject. For example, when someone has an unlisted phone number, their name appears but the phone number appears as “Unlisted.” The individual is making an affirmative notice that they are exercising a privacy right available to them. This puts others on notice that the individual does not want that particular information to be publicly available. If published later in another format, they would be able to show a court why the other party was on notice that this is not public information. It strengthens an individual’s privacy rights by making others very aware that this information is not to be publicly disseminated.

James Ball of *The Guardian* wrote an article about the after-effects of the González ruling. He argued that people no longer see the most relevant information on Google. Instead, they see information that the data subject is not trying to hide. Ball writes that on July 2, 2014, Google removed six *The Guardian* articles from its search results. Ball is concerned that only the rich and powerful who can afford to hire a reputation management consultant will be able to remove all negative traces from search results. Though Google is only responding to

---

122. *Id.*
125. *Id.*
individual requests, it would be the rich and powerful who are expending resources to have the information removed. Ball calls this censorship, even though he admits that the results are still available on The Guardian’s site. The censorship argument is that by removing the results from its search results, Google makes the articles very difficult to find. For example, three of the articles concerned Dougie McDonald, a referee who lied about reasons for granting a penalty in a Celtic versus Dundee United match; he resigned as a result. A user who remembers McDonald’s name would have to know that there is an article available on The Guardian and go directly to The Guardian to search for it. Google will not direct them. However, since Google takes the removal requests literally, if a user searches for “Scottish referee who lied,” the Google results for The Guardian articles remain. This is a chaotic interpretation of the law and the ruling. If McDonald wants to remove those results as well, it truly does allow him to wipe the slate clean. A user could not search for him in Google and would have to go directly to a newspaper to search. However, as the results are currently handled, it implies that relevancy and timeliness of the information are linked inextricably with the person’s name. This places greater emphasis on the name than on the relevancy or timeliness of the information contained in the search results, and that is not the true concern of the González ruling. Under González, the information itself was no longer relevant or timely. González was able to have it removed specifically because it was tied to his name, which gave him standing to challenge the search engine link in court. But the underlying argument was that the information was irrelevant. However, Dougie McDonald’s information may or may not still be relevant. If McDonald is able to have the incident removed from search engines, it is because his name is attached to the information, regardless of whether the underlying information is timely or relevant. The González ruling was not that broad. The question here is whether information about a referee who lied is irrelevant or not timely. It appears Google may not have asked that question. Instead, Google apparently removed information simply because McDonald filed a removal request.

Mahela Khan of the blog Just Cite raises an interesting question regarding the González ruling. She presents an example of a 24-year-old judgment requiring the removal of information from search results. The underlying argument was that the information was irrelevant. However, Dougie McDonald’s information may or may not still be relevant. If McDonald is able to have the incident removed from search engines, it is because his name is attached to the information, regardless of whether the underlying information is timely or relevant. The González ruling was not that broad. The question here is whether information about a referee who lied is irrelevant or not timely. It appears Google may not have asked that question. Instead, Google apparently removed information simply because McDonald filed a removal request.

Mahela Khan, The Right to be Forgotten (Unless You’re Worth Remembering), JUSTCITE (May 16, 2014, 10:48 AM), http://blog.justcite.com/the-right-to-be-forgotten-unless-youre-worth-
old graduate who requests and receives the removal of an irrelevant link
to "an embarrassing photo of a university club he was a member of."  130
However, she then asks: what if this 24 year old later becomes the Prime
Minister?  131 Is there now a public interest in the removed photo?

González himself has become a subject of public interest after this
decision. Therefore, his attempt at obscurity has failed—somewhat
validly, some might argue. According to the court, the details of
González's foreclosure were irrelevant and untimely.  132 However, the
question now becomes whether they are relevant precisely because of
the court battle. That is to say that when someone enters González’s
name in a Google search, one of the most relevant things about González
is his case against Google. However, the fact of the past foreclosure is
the basis for the case. According to Khan, there may now be public
interest in González’s foreclosure that justifies the search result’s
appearance on Google.  133 The courts have not addressed this point.

III. THE HISTORY AND MODERNIZATION OF EUROPEAN DATA PRIVACY
LAW

The basic idea of the right to be forgotten developed from the
French concept of le droit à l’oubli.  134 This phrase translates to “the right
to be forgotten” and is common in French criminal law.  135 The idea is
that once persons serve their time, they deserve a chance to start anew
without their criminal past coming back to haunt them. Some people
have extended the term to online interactions and thought that people
deserve the same right to start anew outside of criminal law
applications.  136

In 1995, the European Commission passed a Data Protection
Directive.  137 This was the first step in securing data protection rights for
European residents. This directive formed the basis for the González
decision involving data privacy rights for individuals.

Currently, a proposed update to the Directive attempts to modernize
the law.  138 The European Commission says these updates are necessary

---

130. Id.
131. Id.
133. Khan, supra note 129.
135. Id.
136. Id.
138. EUROPEAN COMMISSION, HOW DOES THE DATA PROTECTION REFORM STRENGTHEN
for several reasons. The update clarifies the principle for the digital age; subjects non-European companies who offer services to European customers to the law; suggests reversing the burden of proof so that the company must prove the data cannot be deleted because it is still relevant; and creates an obligation for a controller who has made the data public to take reasonable steps to inform third parties that the individual wants their data deleted.  

Many are worried about how the proposal trumps fundamental rights. The European Commission says this is not the case and the right is not absolute. There would still be freedom of expression and the right for the media to report newsworthy events and stories. If the González ruling can provide any guidance for the new proposal, it shows that the courts consider these rights important and they will not allow a user to remove validly posted newsworthy stories simply because they argue for their privacy rights. The González court said the newspaper was not required to remove the results, but Google’s intervening post was an infringing appearance of González’s name.  

On March 12, 2014, a plenary session of the European Parliament voted in favor of reforming the current data protection laws. Currently, officials are discussing various amendments, but there has been no agreement on the amendments as of yet. The European Parliament, the Council, and the European Commission are in discussions over these various amendments in an attempt to construct a law that will apply to all of the European Union. The head of the European Commission, Viviane Reding, has said that there is extremely fierce lobbying on these amendments. A website called LobbyPlag allows people to see which countries and Members of the European


139. EUROPEAN COMMISSION, supra note 8.

140. Id.

141. Google Spain SL, supra note 2, ¶ 62.


Parliament support each amendment. It is ironic that the country responsible for the landmark case regarding online data privacy favors less protection for those seeking online data privacy; however, there is internal debate within the countries providing great variation. For example, Axel Voss, a German Member, is the most opposed to data privacy in Europe despite being from a country that generally favors more data privacy. In short, the proposals of the new Regulation are currently very much in flux.

After the proposals and wording are determined, the next step is for the Council of Ministers to adopt the proposed regulation. When the Ministers have thoroughly discussed and defined its position, it will negotiate with the European Parliament regarding the Proposal. After adoption, the law will go into effect throughout the European Union.

After this point, a determination can be made on whether the information removal forms, such as Google’s, fit within the European requirements. Until then, the form is attempting to comply with a Directive from 1995 that is only now seeing court cases that really challenge the boundaries of the Directive, such as was the case with González. After passage of the new Regulation, there will naturally be challenges in court over new protections. A good example of this is one of the fundamental weaknesses of González. González was able to sue to have the data removed under Spanish law. Google probably complies with the ruling if it removes only the Spanish results. The new regulation may require removal throughout the EU rather than just one Member State. This helps somewhat with the problem of “information hotspots” but does not fully address the problem. European users would still be able to access the United States version of Google to see European blocked search results. Therefore, while the search results are less fragmented, they are still far from uniform.

IV. WHY THE UNITED STATES SHOULD HARMONIZE WITH THE EUROPEAN UNION, AND A PROPOSED TEST FOR DATA REMOVAL

Currently, the law is in a state of flux. González was a landmark ruling regarding removal of an individual’s private data online under certain circumstances, but the ruling will soon be overtaken by the pending regulation proposal in Europe and when the new law is in

---

146. Id.
147. Id.
effect. The González court tried to anticipate the coming changes, but since the law is changing and expanding, it remains to be seen how well the González court anticipated these coming changes. Since there has already been strong influence by American corporations and the proposal would affect American corporations’ duty to remove certain information about European citizens, there is already a need for this to be addressed on a worldwide basis.\textsuperscript{148} The question is how to accomplish this goal practically.

There is no effective means of passing a law that applies throughout the world. On the Internet, a person can communicate and broadcast an idea to many countries at the same time. This is both the promise and the danger of the technology; if it communicates a “worthy” idea, it can reach a large audience and spread quickly. However, the same is true of an “unworthy” idea. Countries are grappling with how to control these unworthy ideas and control the spread of information to and about its citizens.\textsuperscript{149} While there is nothing forcing the United States to pass laws regarding the data privacy of its citizens in online formats, it would be beneficial for the United States to consider the idea and make determinations about what kind of information it wishes to allow its citizens to protect.\textsuperscript{150} Europe has taken steps to consider what freedoms and responsibilities its citizens and corporations should have regarding online data privacy.\textsuperscript{151} The United States and other nations would do well to consider these same ideas and begin to construct laws that allow it not to be stifled in online communications in other nations.

As such, this Article proposes a three-prong test for a person requesting data removal. These prongs may stand alone. That is to say, if the data meets one prong, that alone is sufficient for requiring a site to remove the results. Additionally, websites would benefit under some prongs by allowing users to remove the information themselves, although certainly not in every instance.

The test is as follows: if the information is a private fact that is offensive to a reasonable person and not newsworthy, only the individual may choose to publish the information. Second, if individuals posted the information about themselves or as an expression of their

\begin{itemize}
  \item \textsuperscript{150} \textit{Id.}
  \item \textsuperscript{151} \textit{Id.}
\end{itemize}
opinion, they may remove it or have it removed. This should apply not only to sensitive information, such as financial or medical data, but also to any data the individual chooses to post. Third, if the information is not relevant to the circumstances under which it has been posted or is outdated, and if there is not a compelling reason for it to remain publicly available, then a person may request its removal.

A. Removal of Information a Person Posted About Himself or Herself

First, if the information is a private fact that is offensive to a reasonable person and not newsworthy, it should never be published unless the individual chooses to do so. This is a straightforward rule and the strongest in terms of privacy concerns for individuals. This first prong is also the most inflexible. For sensitive information, if the individual did not post the information, then he or she may demand its removal.

First, private or sensitive information is a subset of personal information. While sensitive information can cause someone to face a loss of reputation, social standing, or even financial loss, personal information is simply information about the person. While all sensitive or private information is personal, all personal information is not sensitive. A good example of the difference between personal and sensitive information is the difference between revealing that someone’s favorite food is pizza and revealing that the person suffers from cancer. While persons are very unlikely to lose a job because they enjoy pizza, persons may lose a job if their employer believes that the company will face higher costs from the lost time, bringing in a replacement, having other employees cover the hours, or increased health care costs for the employer. In another example, a person is unlikely to be ostracized from his or her community if his or her favorite color is green, but may face a strong backlash from his or her neighbors if he or she voted for a political candidate that is unpopular in the area. These examples show how private information is a part of personal information and why the distinction between personal and sensitive information is important to draw. The first prong would only protect information that could result in a loss to the person whose privacy is being violated, which is why only private information must be removed.

The first prong is recognized essentially in the tort of “publication of private facts.” Of all the American laws, this tort is best situated to

allow U.S. citizens the right to remove true information about themselves from online sources. In this tort, an action exists for publishing private facts about another person, even if the facts are true.\textsuperscript{153} Unlike defamation, the truth does not bar recovery.\textsuperscript{154} The elements of the tort require there be a public disclosure of a private fact that is offensive to a reasonable person and not newsworthy, similar to the requirements of the first prong.\textsuperscript{155} A public disclosure is necessary to the tort and the first prong because it shows the violation of the individual's privacy. There is a big difference between communicating a fact to one person and telling the world at large.

Next, there must be a disclosed private fact. Usually, if the individual has disclosed the information previously, it is not a private fact. For example, in \textit{Sipple v. Chronicle Publishing Co.},\textsuperscript{156} a man who stopped an assassination attempt on President Ford sued two newspapers for revealing he was a homosexual.\textsuperscript{157} The court denied his suit because he was well known in the gay community; therefore, his sexual orientation was not a private fact. If something is publicly known, then it is not a private fact.\textsuperscript{158}

The third element is whether the publication would reasonably offend a person of ordinary sensibilities. This examines whether it is reasonable to expect that the information should remain private. While most people would not be offended that someone publicly revealed they prefer Pepsi to Coke, many people of ordinary sensibilities would be offended if their exact voting records for the last Presidential election were made public; we expect such information to be kept private. The distinction between personal and private information has already been discussed, but there is also some difference between private information and sensitive information. Private information includes information that is typically protected by privacy laws such as health care\textsuperscript{159} and employment information. Sensitive information is information that has been disclosed to others but that they may prefer not be told to anyone.

\textsuperscript{153} \textit{Id.} (listing elements of this tort).

\textsuperscript{154} \textit{Id.}; cf. \textit{Gertz v. Robert Welch, Inc.}, 418 U.S. 323, 375 (1974) (emphasis added) ("the ordinary citizen could make out a prima facie case without proving more than a defamatory publication and could recover general damages for injury to his reputation unless defeated by the defense of truth").

\textsuperscript{155} \textit{Id.}

\textsuperscript{156} \textit{Sipple v. Chronicle Publ'g Co.}, 201 Cal. Rptr. 665 (Cal. Ct. App. 1984).

\textsuperscript{157} \textit{Id.} at 667.

\textsuperscript{158} \textit{Id.} at 671.

else. This could include information about details of a person's domestic life. In both sensitive and private information, there are facts that some people may not want shared. However, this prong is constructed to allow certain private or sensitive information to be shared while keeping that which most people would find offensive from being publicly shared. That is where this element becomes instructive. Thus, private information and sensitive information are used interchangeably because each contains a higher likelihood of risk that there will be something that should not be shared when compared to personal information. It is a fact-based question whether or not a person of ordinary sensibilities would be offended by the disclosure.

Fourth, the information cannot be newsworthy. There are occasions where the information can fit the first three prongs and still fail on the fourth. For example, when former President Bill Clinton had an affair with Monica Lewinsky, the affair was a private fact. When made public, the second element of a public disclosure was met. A reasonable person would be offended by having their private sexual activities made public, which meets the third element. The problem is that in most cases, the courts generally rule that the details of the private lives of prominent figures are newsworthy. In this instance, although Lewinsky would possibly want the details of the affair removed from online, the story is newsworthy, and it would remain under the first prong due to the newsworthiness.

Nationally, this prong is important because not all states recognize this tort. By recognizing a national right for individuals to remain private, the law can apply throughout the United States. This is important when applied to the Internet. For example, Indiana does not recognize the tort of publication of private facts. If a resident of Missouri posts information about a resident of Indiana on the internet and there are not enough minimum contacts to provide jurisdiction in Missouri, the Indiana citizen may not be able to recover. While most areas of the law have had to navigate jurisdictional

---


161. Id. This Article does not consider jurisdictional questions but provides this example to show how laws in different states could have different results. For example, this Article does not discuss whether Missouri law views the "effect" of the tort in Missouri or whether jurisdiction would result because the Indiana publisher's intent was to channel the effect into Missouri.

162. Id.
issues such as this for many years, it is difficult to argue that imaginary borderlines should apply to the Internet because of its initial purpose.

Internationally, this is still true. If a different regulatory format is applied and different search results occur based on the location of the person performing the search, then it threatens to chill international communication because of the inconsistency of data that varies based on location. Results that are even more unusual can occur when a person who is a resident of the United States signs into his Google account while on vacation in Spain. Which jurisdiction is he subject to—the Google results of his home jurisdiction where the account is based or the Google results of the country where he is presently located?

An example of the way this prong works in practice is if Person A posts that her brother was diagnosed as HIV positive on Facebook and the brother discovers the post and requests that Person A remove the post immediately or reports it to Facebook, Facebook should suppress the post until further examination. If Person A does not willingly remove the post, the brother could sue Person A seeking an injunction requiring removal of the information. Preferably, the website would be joined under Federal Rule of Civil Procedure 19(a)(1)(A)\textsuperscript{163} to allow for the opportunity for complete relief to the brother. A court would examine the elements to see whether the post fits the first prong and would ultimately order its removal and any damages the person is entitled to because of the posting.

In the González ruling, the court noted that individuals could request removal of private information when the information is not newsworthy. Much of the ruling discussed how González was entitled to data privacy; however, the court specifically noted that in some instances, there might be newsworthy reasons to make the information publicly available.\textsuperscript{164}

Critics argue that allowing someone to remove items about them curtails freedom of speech.\textsuperscript{165} However, freedom of speech is subject to other considerations. For example, dignitary torts such as defamation and the publication of private facts restrict what a person may say or write.\textsuperscript{166} These torts limit speech that goes too far and violates a person’s

\textsuperscript{163.} FED. R. CIV. P. 19(a)(1)(A).
\textsuperscript{164.} Google Spain SL, supra note 2, ¶ 17.
dignity. Therefore, curtailing freedom of speech already exists, and this prong merely solidifies the idea that it applies to online communication in the same instances as already exist.

B. Removal of Information Another Individual Posts

On the second prong, if an individual posts information about himself or as an expression of his opinion, he should be allowed to remove it. If he has control over the website, this is easy: the user simply removes it. However, what if a person was considered the website owner but did not actually have control over the website? The letter that Cleveland Cavaliers’ owner Dan Gilbert posted on the Cavaliers’ website to fans when LeBron James left Cleveland for the Miami Heat in 2010 is an example.168 When speculation arose that LeBron James would return to the Cavaliers, the letter disappeared from the website.169 However, let us assume it remained and Gilbert wanted it removed. As the owner of the team, many consider Gilbert the website owner. However, it is unlikely he has actual control over the website. Gilbert would have to prove to a court why he has the right to remove the data because it is no longer relevant. Under the second prong, Gilbert should have the right to remove information he posted.

However, there is a second problem with that example. Gilbert would need to prove that he posted the information about himself. While the letter is widely seen as a letter to the fans about LeBron James, Gilbert would need to prove that the letter is really about his own feelings when James left the team. Due to his promises to the fans and expression of opinions, it should be easy to prove to the court that Gilbert’s letter is really about himself.

However, what if the letter was not an expression of Gilbert’s opinion? What if someone wrote a letter or article about another individual, posted it on his or her own website, and wanted to remove it? While there should be protections in place, the second prong is not meant to extend that far. Many other considerations can come into play when considering removal of the article. For example, defamation may arise, and the deletion may be spoliation of evidence. If Gilbert posted

167. Id.
on the Cavaliers website, “LeBron James cheated throughout the entire time he was with the Cavaliers,” and assuming it was untrue, then James could sue Gilbert for defamation. If Gilbert destroyed the evidence by removing the claim from the website, it could make it difficult for James to prove he had been defamed without expensive recovery of archived data on network servers or internet archives. Just because the information has been removed does not mean that the person’s reputation is restored. The individual may still suffer the same negative effects to his reputation. Because of examples such as these, the second prong should not be extended to situations where one individual is posting anything other than his own opinion on his website about another individual.

The Gonzalez ruling has wrongfully been applied already to block an article that one person wrote about someone else. Robert Peston is an economic editor for BBC. He received a takedown notice on July 2, 2014, from Google in response to Gonzalez that read, “(n)otice of removal from Google Search: we regret to inform you that we are no longer able to show the following pages from your website in response to certain searches on European versions of Google.” Google then cited the specific page in question. The piece in question was a 2007 article about Merrill Lynch and its former boss Stan O’Neal. However, neither Merrill Lynch nor Stan O’Neal appear to have instigated the removal. Peston says it appears that someone who posted a comment to the article sent a complaint to Google. As a result, Google slated the article for removal. As of July 3, 2014, Peston says the article is still visible in search results if one enters the name “Stan O’Neal.” However, when a user enters the name of the person who left the comment, the article no longer appears.

Essentially, this is exactly why the second prong is necessary. One comment that a user made and later regretted threatened to take down an entire article. If the entire article was removed, then it could be used to circumvent applicable laws. For example, suppose that O’Neal was under investigation for his activities at Merrill Lynch. The information contained in the article is arguably still relevant and timely. However, a

171. Id.
172. Id.
173. Id.
174. Id.
175. Id.
user could argue his comment is not. If Google's standard policy was to remove the entire article, then O'Neal could leave a comment to the article that is irrelevant to his actions at Merrill Lynch and then request removal since it was not relevant. Google would operate under its standard policy of removing the entire piece, and O'Neal would accomplish indirectly what he could not directly. Just as loathsome is the idea that one comment is sufficient to support a request to remove an entire article. By using the second prong, an individual may only remove what they posted about themselves or their own opinions on a matter.

Finally, although the second prong certainly should work in conjunction with the other prongs, it has a special connection to the first prong. In the first prong, if the information is in a sensitive category such as health information or voting records, the information should never be published unless the individual chooses to do so. However, if persons decide to post that information themselves on their own website, they may later choose to remove it. This means that although a doctor may not post someone's health status online, individuals may post their own information and then later choose to remove it if they wish to do so. This recognizes that individuals may decide to post on Facebook that they are having surgery and then later change their mind about giving details.

Where the two prongs provide even greater privacy protection is when someone posts about another individual's health information. For example, suppose a daughter posts on Facebook that she is worried about her mother's upcoming surgery. The mother did not want to make her surgery public. Suppose that a family argument ensues because the child claims the right to post whatever she wants on her own Facebook status, and the mother claims the right to privacy in her healthcare information. The daughter may claim that she is expressing her opinion and feelings about her mother's surgery, and under the second prong this would be valid. However, the first prong allows the mother to have the information removed. The information is private, and the mother may have it removed.

Despite attempts at harmonization, there is room for each country to decide how far it would like the laws to extend. This is true even under González—the court applied the Spanish laws. Even though there is currently a minimum standard set throughout the entire EU, the countries can decide to exceed the minimum standards and offer their citizens greater privacy rights. Therefore, in the proposal, some countries have strong paparazzi laws, and the country may determine that gossip
websites cannot post photos of a person without the person’s consent. Other countries may decide that it is permissible. Some may prohibit a discussion on the health of the President or Prime Minister where other countries may have a valid public reason to discuss the health of those leading the country. While these may lead to situations where some information is available in some areas but unavailable in others, this is a limited occurrence. Currently, paparazzi laws already vary between different countries and the courts of these countries have navigated the differences. Second, the health of a local politician rarely raises enough interest in areas the politician does not serve. Simply put, those in the United States may not care about the health of the British Prime Minister. Therefore, if the results were available in the United States and blocked in the United Kingdom, the resulting harm is low. Some would argue that if the individual does not care about the information, they should not be entitled to access it. However, this does not account for individual areas of interest. Completely blocking the information means it would not be accessible to those who do care about it, such as someone writing or reading a blog on current international affairs. In practice, by blocking information, it essentially requires an individual to show evidence that he needs access to a particular fact before that individual can access that fact. This slows the spread of factual information throughout the world.

C. Removal of Outdated or Irrelevant Information

González shapes the third prong substantially. This is the most complicated of the three prongs because it contains two subparts. First, in order to remove the information, it must be determined to be irrelevant or outdated. In both the European Union and the United States, the first party to make the determination will be the search engine, and ultimately courts will review the determination. Second, there must be no compelling reason for the information to remain publicly available. Though these subparts have a great deal of overlap, both are necessary because of very limited situations where information under the González analysis could be considered irrelevant and outdated, but there is still a compelling reason why the information should remain

available. To understand why, each element must be examined in detail.

Part A of the third prong is that if the information is not relevant to the circumstances under which it has been posted or is outdated, it should be removed. There are two conditions in this portion, and if the circumstances show the information is outdated or irrelevant, then the information should be examined under Part B to see whether it applies. There is no need to meet both conditions; if a person can prove that it meets either, it will be sufficient to continue the analysis. While González was both irrelevant and outdated as it related to Google’s posting of the information, it is not required for the information to fall under both.

The reason it should meet either condition, and not necessarily both, is to allow for greater data privacy. Often, timeliness is an important characteristic in determining whether something is relevant. However, the reverse is not necessarily true. For example, assume the González case was not Google indexing a newspaper article that was posted many years earlier. Instead, assume the newspaper simultaneously published a paper and digital edition of the newspaper. The exact same information was listed in each. Google indexed the website, and it was added to search results less than a minute after the newspaper posted it. This means the auction has not occurred yet. Applying the same analysis to this situation as the court applied to the facts, the newspaper stands in the same position in the modified facts as it does in the actual facts. The information was relevant and timely when posted. However, Google is in a different position. Rather than failing on both timeliness and relevance, Google posted timely information. The foreclosure is pending, and the auction will be held immediately. Therefore, the information is certainly timely. Nevertheless, it is not necessarily relevant. By applying its algorithm, there is still not a relevant tie between González’s name and the fact that he has a foreclosure, absent any other search terms. To find the information relevant, the court would need to determine that there is a valid reason why the website’s algorithm determined that this is such an important fact about González that it should show up in the first page of search results about him. That is where Part B comes into play. There very well may be compelling reasons why it should appear that high in the search results. However, that will be a fact to prove at trial.

This leaves Google with a problem. Now it must show a purpose for posting the information it posts. Under the modified facts above, it is unlikely that Google can honestly say it is attempting to drive more buyers to the auction, especially if it displays the search results outside
of the immediate area. However, if it only displays the results in the local area, it leads to the problem of creating various information zones. González could object that the information is irrelevant if displayed in the United States, but if Google does not display the information, it creates a variable internet with search results available in some places and not in others. This generally should be avoided unless Google makes it clear that the information is locally based. This tells the user knowledge about the source of the information and the scope of that information. A solution such as “Google Local” would be a good solution to providing localized information.

“Google Local” would be an option the user selects, similar to choosing Google Maps or Google Calendar. Everything that appears under this section is limited to a specified geographic location. Therefore, the results would tell the user that everything they are viewing is limited to a 1, 5, 25, or 50 mile radius of the user’s IP address. Alternatively, Google could allow the user to specify the radius. For example, a user in western Iowa may wish to have a wider geographic area be “local” than a person in New York City. All information that appears in the Google Local listings would be limited to that preselected geographic scope. All information on the normal Google page would remove that information that is relevant only to those in a particular geographic location.

Part B of the third prong requires removal in the absence of a compelling reason for public availability. Stated conversely, if there is a compelling reason for the information to remain publicly available, it should not be subject to a successful removal request. This is much more common than a situation where information is only relevant or only timely but not the other. This situation can arise when there is information that is not relevant to the circumstances under which it was posted and is not timely, but there is a compelling reason for the information to remain. Under the modified facts above, the newspaper has relevant and timely information. There is a compelling reason to post the information, which is to bring people to the auction. Therefore, the information does not have to be removed from the newspaper’s website. Google still faces a different analysis. The court will need to examine whether there is a compelling reason why the information ranked so highly in the search results. As noted above, it would behoove Google to create a local results section. After all, Google and other search engines already offer local results. This increases its brand offerings and demonstrates a commitment to expansion of that offering while making it clear to users that the search results have a limitation in scope. If it
does not, then almost any search result is open to a question of relevancy. Google’s purpose is to generate search results. However, by creating a local search results section, Google is much closer to being able to argue that it has a compelling reason for posting the information. It is bringing local news and search results to local residents. If González argued that Google’s local results were irrelevant, then Google will only have to show how the results are relevant locally. Perhaps by limiting the geographic area, Google can argue that a local user searched for González by name, and these were the only results that appeared locally. This puts Google much more in line with the newspaper’s legitimacy in publishing the data by limiting the geographic region.

The scope of the geographical limitation is hard to define. In some cases such as New York City, it may be appropriate to divide the local area to neighborhoods. In rural areas such as western Iowa, the local area may be expanded to include the entire western half of the state. In areas such as Kansas City, the local area may encompass an area that extends between Kansas and Missouri. The local area would be based on what a local user would consider geographically close.

The idea of having a “Google Local” does not offend the idea of a unified Internet since it is only a limited option that a user may choose. Just as a person in the United States may read a newspaper that is located in Britain, one may have to put additional work into finding out information that is not local to them. If a user in the United States wanted to search Google Local for Mario Costeja González, nothing would appear about the foreclosure or man in Spain. If the U.S. user adjusted his settings to display local results for a particular region of Spain, González would appear. The results are not invisible. Instead, it acknowledges that the information is irrelevant outside of that area of Spain. If a person in the United States does change their settings to show only results in a particular area of Spain and searches for Mario Costeja González, then the courts can infer relevancy. This does not offend the González ruling because a person performing the search has taken affirmative steps to look for a person outside of his country by that name and acquire information about him. Thus, the search is relevant on its face because of the steps the user has taken to search for someone by that name in that particular region.

Currently, Google’s form for information removal says that it “may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of
government officials.” However, while this information is certainly compelling and the González court recognized a need for Google to post compelling information, one must wonder if this is narrowly tailored to fit the court’s ruling. For example, say that Peter Smith is a surgeon in Des Moines, Iowa. He is accused of malpractice, and the patient that sued him was awarded $1.2 million in damages for a botched surgery. The Des Moines Register reported the lawsuit and outcome, and Google indexed the results worldwide. The newspaper may post the information online since it was relevant and timely when posted. However, Smith may sue Google for posting the link saying that it is not relevant or timely. If the lawsuit and judgment only occurred a few weeks earlier, Google may not have a timeliness issue. It will refuse to remove the results saying that there is a compelling reason to keep the link—namely that there has been professional misconduct. Additionally, the public has a compelling reason to search for this doctor and anything that may affect their decision to use him as a surgeon. However, Smith will counter that there is no compelling reason these results should be available worldwide. In other words, there is little reason that someone typing the name “Peter Smith” in Britain would need to know of a Des Moines, Iowa surgeon. Thus, it is back to a relevancy question. Because of this reason, the Google form requesting removal may need further refinement to specify exactly what will be removed under what circumstances, and what sort of information will be available in which locations and for what purposes. Currently, the form is simply too vague.

V. CONCLUSION

The Court of European Justice ruled that González’s information was timely and relevant when posted on the newspaper’s website because it told of factual events of a foreclosure that were relevant when posted. However, the Court of Justice of the European Union found that Google’s determination that this was worthy of appearing in the first page of search results when a user searched for González was not relevant or timely. The information on Google did not drive any additional buyers to the foreclosure sale that happened over a decade earlier. It did not notify a searcher that González was currently having any financial difficulties. The information was no longer relevant and timely, and González was entitled to have the link removed from Google.

178. Search Removal Request, supra note 5.
search engines. Because there was no compelling reason for the information to remain available, Google had to remove the link.

As a result, Google and other search engines have taken steps to allow users in the European Union to request removal of data that is no longer relevant or timely. This is not an absolute right, for example, when there is a compelling reason for the information to remain available such as information that Google deems to be in the public interest. However, Google will almost certainly face challenges to its information removal request procedure as new cases give further guidance about the boundaries of the law.

One event that may cause radical changes in the data removal request form is a new directive that is being discussed in the European Union. The representatives of the various Member States of the EU have pledged that they will pass a new regulation, but they are currently debating the details the new regulation will take. It currently appears that it gives stronger privacy rights to individuals and will increase fines on companies that refuse to remove information that individuals will be allowed to have removed from the Internet. Some nations want stronger protections than others, and even American corporations are lobbying for changes because they will be heavily affected by any potential fines.

The corporations, especially search engines, should take similar steps. Even if the United States is unwilling to create a law, the search engines can be sued in foreign countries to remove certain links. If the search engines want the information to be consistent across the entire world and not create "information hot spots," then the steps the EU takes will create a de facto law in the United States as U.S. corporations comply with foreign rulings. Search engines such as Google may choose to allow such information hot spots, but market the idea as a beneficial feature rather than a detriment. By presenting local search results and including information such as names and news that is only targeted towards a certain locality, the search engines comply with the law and also respect that information in certain instances is relevant only within a certain locality.

Nations considering implementation of an information removal law should consider the three-prong test proposed above. First, if the information is the publication of a private fact that is offensive to a reasonable person and not newsworthy, that information should never be published unless the individual chooses to do so. Second, if individuals posted the information about themselves or as an expression of their opinion, they should be allowed to remove it. Third, if the information is not relevant to the circumstances under which it has been posted or is
outdated, and if there is not a compelling reason for it to remain publicly available, then that information should be removed. Any of the three prongs would be a sufficient basis for removal of the information.

The first prong provides that others should not post private, offensive material about another. That individual may choose to post it himself, but if another posts the same information, the data subject may successfully request its removal. The second prong allows people to state information about themselves or their opinions, reconsider, and choose to have the information removed. This would allow someone who posted an opinion, thought, or information about himself to decide that they unwisely posted something and now wish to retract it. The third prong implements the González ruling by determining that if the information posted about a person is irrelevant or untimely and there is not a compelling reason for the information to remain publicly available, then it should be removed.

Passing laws that are similar to the proposed three-prong test would allow a nation to respect an individual’s right to privacy, but not allow them to evade all mention on the internet. If a politician commits some act that is of public concern, then the public has a valid reason to discover this information. Nations would benefit from such laws by setting clear boundaries for what information should be private and what should remain publicly available. Corporations would benefit by having a consistent law applied throughout the world and knowing the definite laws that will apply, no matter where the information appears. Individuals would benefit from such laws by having an ability to remove irrelevant, untimely, or embarrassing information that is not within the public interest and by having a definite means of enforcement for the removal of such information. All three entities—nations, corporations, and individuals—benefit by having a consistent Internet that displays the same information, regardless of jurisdiction, unless the user has a clear reason to expect that the information they are viewing is only relevant in the locality where it is viewed.