The Internet (Never) Forgets

May Crockett

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation

May Crockett, The Internet (Never) Forgets, 19 SMU SCI. & TECH. L. REV. 151 (2016)
https://scholar.smu.edu/scitech/vol19/iss2/4

This Comment is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
The Internet (Never) Forgets

May Crockett

I. INTRODUCTION

Our memory is hard to conceptualize. We remember some things, while we forget others. Some memories remain crystal clear, while some slowly fade away into the past. Our memories are like books at the public library; they remain on the shelf, but soon become worn down or simply lost. What causes us to forget is not totally clear, but a recent Stanford study suggests that our brains are meant to forget.¹ In fact, we would not be able to get through our day if we didn’t forget.² However, the Internet and social media have caused some memories to become harder to forget, which begs the question: shouldn’t some of those things be forgotten?

Whether we like it or not, we now live in a world where the Internet records everything we do. Facebook alone has nearly 500 million members who spend 500 billion minutes per month on the site.³ The average Facebook user shares 25 billion pieces of content each month and creates 70 pieces of content each month.⁴ These online records show over a decade’s worth of decisions which, unlike those in our brains, cannot be forgotten. Where our memories fade, the Internet never forgets. At the drop of a hat, friends, family members, acquaintances, and even strangers can call up these records, and worse, they can use them against us.

There are countless examples where the Internet can get you fired, ruin your career, or even cause employers to snub you before the job interview. A recent survey outsourced by Microsoft shows that seventy-five percent of U.S. recruiters and human resource professionals perform online searches of possible candidates.⁵ One victim of this phenomenon is Stacy Snyder.⁶ When Snyder was twenty-five years old and training to be a teacher, she posted a

---


2. Id.


4. Id.


* May Crockett is a 2017 candidate for a Juris Doctor at SMU Dedman School of Law.
MySpace photo of herself at a party. She was wearing a pirate hat and holding a red solo cup with the caption “Drunken Pirate.” The Dean of Snyder’s school said that she was promoting drinking and as a result, denied Snyder her teaching degree upon graduation. Though Snyder sued, the court found that her “Drunken Pirate” post was not protected speech.

Another instance occurred when a Canadian therapist was crossing the U.S. border to pick up a friend from the Seattle airport. The border agent searched his name and found that five years earlier he wrote in an academic journal that he took LSD sometime in the 1960s. As a result of this discovery, the border agent did not allow the Canadian therapist to enter the United States. These are just a couple of examples of how the Internet’s expansive memory has negatively affected individuals. So what do we do about this extensive, haunting, permanent, online record of our lives?

In the popular movie The Dark Knight Rises, Catwoman has an extensive criminal history of jewelry stealing and more. Desperate to erase her past from any database, Catwoman sells Batman’s fingerprints in exchange for a “clean slate.” However, the buyer did not keep his side of the bargain. Instead, Batman acquired the clean slate tool to keep it out of “the wrong hands.” He later offered the clean slate tool to Catwoman, in exchange for her assistance in saving Gotham City. Catwoman then had the power to erase her past from any database online, erasing all reports of her criminal history and past misconduct.

Although the clean slate tool seems unrealistic, a similar idea called “the right to be forgotten” has become an internationally debated issue. The right to be forgotten deals with the ability to control what personal data or infor-

7. Id.
8. Id.
9. Id.
10. Id.
12. Id.
13. Id.
15. Id.
16. Id.
17. Id.
18. Id.
The Internet (Never) Forgets

Information is accessible through search engines and other websites.\(^{20}\) With the right to be forgotten, one could request a search engine to remove certain data that appears when someone searches their name.\(^{21}\) But along with this power comes serious implications. Just as in *The Dark Knight Rises*, we must consider the negative effects of the right to be forgotten.

The Internet has become a prevalent part of our lives and our ability to access information has increased exponentially. Thus, the United States will soon have to consider the pros and cons of the right to be forgotten. Currently, U.S. citizens have no right to be forgotten.\(^{22}\) The United States places more weight on the First Amendment then the right to privacy inherent in the right to be forgotten.\(^{23}\) But should we extend the right to privacy to include a right to be forgotten in certain instances? This national debate has increased in light of a recent European Union (E.U.) decision, which established the first-ever right to be forgotten.\(^{24}\) Now countries including the United States are being forced to consider whether to adopt this right to be forgotten into their legal framework. There is no clear answer to whether there should be a right to be forgotten in the United States, but this comment will provide a comprehensive review of the field.

To understand the history of the right to be forgotten, this comment will first look at cases from other countries including Germany, Argentina, and Spain. Further, this comment will provide an extensive overview of the progression of the right to be forgotten in the E.U., which includes the general right of privacy in the E.U. as protected by the Data Protection Directive of 1995 (Directive).\(^{25}\) The landmark decision of *Google Spain SL, Google Inc.* v. *Agencia Española Protección de Datos and Mario Costeja González* (*Google v. AEPD*) interpreted that right,\(^{26}\) and the proposed General Data Protection Regulation (GDPR) clarified it.\(^{27}\) The E.U.’s history, legislation, and judicial decisions establish a right to be forgotten. After analyzing the right with a global perspective, this comment will focus on the real issue: should the United States adopt the right to be forgotten? Analysis of the

21. Id.
22. Id.
23. See id.
United States’s background in privacy law, the arguments on each side of the issue, as well as practical implications of the right to be forgotten will determine not only whether the United States should adopt the right to be forgotten, but more importantly, whether the United States will adopt a right to be forgotten.

II. WORLDWIDE HISTORY OF THE RIGHT TO BE FORGOTTEN

The right to be forgotten is a worldwide issue.28 Many countries are facing claims brought by citizens asking them to remove information from the Internet.29 Citizens are asking for the right to be forgotten.30 The cases discussed in this section from Germany, Spain, and Argentina show how this issue arises and how those courts handled it in the past.31 Although some of these cases were decided decades ago, they are still representative of the underlying issues present today. In these cases, the lower courts tend to rule against the search engines, but the higher courts usually reverse the lower court’s ruling.32 These decisions represent the constant battle between the freedom of expression, press, speech, the right to privacy, and the overall need for a worldwide clarification on the right to be forgotten.

A. Germany

On October 27, 2009, lawyers for Wolfgang Werlé and Manfred Lauber sent Wikipedia a cease and desist letter, requesting removal of their clients’ names from the German and English Wikipedia pages of Walter Sedlmayr.33

30. See id.
32. See id.
In 1993, a court found these half-brothers guilty of murdering their former business associate, Walter Sedlmayr.\(^{34}\) They tied him up, stabbed him in the stomach, and beat him on the head with a hammer.\(^{35}\) The half-brothers’ lawyer relied on a 1973 ruling that allowed the suppression of a criminal’s name in news accounts once he or she has paid his debt to society.\(^{36}\) However, no one had yet applied this concept in the context of the Internet.\(^{37}\) After winning a default judgment against Wikipedia for one of the men, the lawyers fought for their other client, contending that his “name and likeness cannot be used . . . in publication regarding Mr. Sedlmayr’s death.”\(^{38}\) In the cease and desist letter, the lawyers stated:

> Our client has served 15 years of his life sentence for murdering Mr. Sedlmayr in 1990. He has been released on parole in August 2007. His rehabilitation and his future life outside the prison system is severely impacted by your unwillingness to anonymize any articles dealing with the murder of Mr. Sedlmayr with regard to our client’s involvement.\(^{39}\)

The cease and desist letter additionally demanded legal fees and compensation for “emotional suffering.”\(^{40}\)

The German court had to decide whether the 1973 decision applied in the Internet age, excising legally published names from archives.\(^{41}\) In 2008, a Hamburg Court found that the 1973 decision did apply to the Internet and ordered German Wikipedia editors to remove their names.\(^{42}\) However, in 2009, the German Constitutional Court reversed the lower court’s decision, deeming it an imposition on the freedom of press.\(^{43}\) The Court ruled that the


\(^{35}\). Id.

\(^{36}\). John Schwartz, German Killers Demanding Anonymity Sue Wikipedia’s Parent, N.Y. TIMES (Nov. 12, 2009), http://www.nytimes.com/2009/11/13/us/ 13wiki.html?_r=0 (Wikimedia’s response to Stopp’s cease and desist letter questioned the relevance of German law given that they had no operations or assets in Germany).

\(^{37}\). Id.

\(^{38}\). Id.


\(^{40}\). Id.; Letter from Dr. Alexander H. Stopp Rechtsanwalt, supra note 33.

\(^{41}\). See Schwartz, supra note 36.

\(^{42}\). See Bruhn, supra note 31.

\(^{43}\). Id.
half-brothers should expect some intrusion into their privacy in relation to the public interest and freedom of press. The German and English Wikipedia pages about Walter Sedlmayr currently contain the half-brothers’ names. This case is a prime example of a specific group of people who in the past have requested a right to be forgotten—criminals. The opposing arguments presented in this case address criminals’ right to delete their criminal history in order to effectively re-enter society after they have served their time. On the other hand, there is the argument that granting criminals this right to erase their criminal history may distort history. Historically, an individual’s criminal history has been easily discoverable; however, with a right to be forgotten we may never know who murdered Walter Sedlmayr.

B. Argentina

Meanwhile, in Argentina, actresses, models, and athletes have filed hundreds of complaints against Google and Yahoo to remove search results and links to photographs. The most famous of these complaints is that of singer, actress, and model Virginia Da Cunha. Da Cuhna claimed that her personal search results, which connected to other websites offering pornography, escorts, and other adult material, harmed her career and overall image. The lower court judge, Judge Simari, found that the right to control one’s personal data included the right to prevent third parties from using one’s image. Judge Simari ruled in favor of Da Cuhna and ordered Google and Yahoo to pay 50,000 pesos as compensation for her moral damages. Additionally, Google and Yahoo had to remove Da Cuhna’s search results related to implicitly sexual activities.

However, the Federal Civil Appellate Court, in a two to one decision, reversed the lower court. The appellate court ruled that Google, Yahoo, and other search engines should not be responsible for instances where third par-

44. Id.
45. Walter Sedlmayr, supra note 34.
47. Id.
49. Id. at 24.
50. Id. at 26.
51. Id. at 28.
52. Id.
53. Id. at 28–30.
ties had posted Da Cuhna’s photo on sexual websites. But the opinion of
the appellate court did not take a definitive stance on the right to be forgot-
ten. While the court defended Google and Yahoo, stating that although “re-
membering” has become the norm in the digital age, they also stated that
there is value in forgetting.55

There are over a hundred cases similar to Da Cuhna’s pending in Argen-
tina. Entertainers, models, and other individuals bring these cases to request
the removal of user-generated content. These cases include Sports Illus-
trated swimsuit model, Yesica Toscanini, and soccer player, Diego
Maradona. Both Google and Yahoo’s counsel argued that the search en-
gines cannot be held liable for third-party content or association with a sexu-
ally related website.59 But what if Argentina had an explicit right to be
forgotten? Would Google and other search engines have to remove this user-
generated content as requested by models, actors, and other individuals?

C. Spain

In Spain, the Agencia Española de Protección de Datos (AEPD), or the
Spanish Data Protection Agency, handles privacy complaints.60 Since around
2010, complaints from the public about their representation have increased
each year by approximately seventy-five percent. In 2011, Google was or-
dered to remove links to articles in several prominent newspapers as a result
of these complaints. There were approximately 100 complaints brought
before the highest court in Europe to clarify these privacy laws.

55. Id. at 30.
56. Jeffery Rosen, The Right to Be Forgotten, 64 STAN. L. REV. ONLINE 88, 91
(2012).
57. Id.
58. Vinod Sreeharsha, Google and Yahoo Win Appeal in Argentine Case, N.Y.
59. See id.
60. Josh Halliday, Google to fight Spanish privacy battle, THE GUARDIAN (Jan. 16,
2011), http://www.theguardian.com/technology/2011/jan/16/google-court-
spain-privacy.
61. See id.
62. Id.
63. See id.
One of the complainants was Hugo Guidotti Russo.\textsuperscript{64} The complaint dealt with his personal search results, which included a 1991 news article about a malpractice claim involving an alleged botched breast surgery.\textsuperscript{65} The article, however, does not mention Russo's acquittal.\textsuperscript{66} Russo contends that this twenty-year-old article involving legal and personal information should not be deleted from the original source but removed from Google search results.\textsuperscript{67} Russo's complaint was one of eighty complaints in which the Spanish Data Protection Agency told Google to remove personal information about individuals from its search results.\textsuperscript{68} Another complaint dealt with a man who wanted to erase his search results about decade old attachment proceedings.\textsuperscript{69} The latter complaint led to the establishment of the right to be forgotten in the E.U.\textsuperscript{70}

Overall, Spain has strictly enforced an individual's right to privacy.\textsuperscript{71} Only a few years ago, Spain was the only country where a search engine could be forced to remove links to websites that did not contain illegal content.\textsuperscript{72} Spain's overall idea of privacy as applied to the latter complaint led the E.U. to an overhaul of their privacy rights.\textsuperscript{73} This overhaul included the evolution of the right to be forgotten.\textsuperscript{74} As reported by The Wall Street Journal a few years ago, "A movement has cropped in parts of Europe to create a 'right to be forgotten,' which would let individuals excise personal information from the World Wide Web on privacy grounds. The European Commission, as part of its data-protection overhaul, has proposed recognizing such a


\textsuperscript{65} Id.

\textsuperscript{66} Id.

\textsuperscript{67} Max Colchester et al., Plastic Surgeon and Net's Memory Figure in Google Face-Off in Spain, \textit{The Wall St. J.} (Mar. 7, 2011), http://www.wsj.com/articles/SB10001424052748703921504576094130793996412?cb=logged0.9696249715052545 (subscription required).

\textsuperscript{68} Id.

\textsuperscript{69} Ashifa Kassam, Spain's everyday internet warrior who cut free from Google's tentacles, \textit{The Guardian} (May 13, 2014), http://www.theguardian.com/technology/2014/may/13/spain-everyman-google-mario-costeja-gonzalez.

\textsuperscript{70} Id.

\textsuperscript{71} Colchester et al., supra note 67.

\textsuperscript{72} Id.

\textsuperscript{73} See id.

\textsuperscript{74} See generally id.; Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.
right." This evolution will be examined in detail throughout the following section.

III. THE EVOLUTION OF THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION

The E.U. places great value on personal honor. These values were "born out of the 19th Century French and German legal protections that once permitted honor-based dueling." This personal honor has been translated to strong protection of the right to privacy. As stated in the novel, *Who Controls the Internet?*, "For many purposes, the European Union is today the effective sovereign of global privacy law." This high regard for privacy resulted in the general expansion of privacy laws to include the right to be forgotten. The right to be forgotten "can be considered as being contained in the right of the personality, encompassing several elements such as dignity, honor, and the right to private life."

The E.U. protected this right of privacy before the Internet through the Directive, which was passed in 1995. But as technology, and particularly the accessibility of personal data on the World Wide Web, increased, the E.U. had to consider the Internet's implications for the Directive. With the landmark decision of *Google Spain v. AEPD*, the E.U. officially recognized that the long standing right of honor—or the right to be forgotten—applies to the Internet. This case marks the origin of the right to be forgotten in relation to the Internet. Not only did this decision officially create a right to be forgotten, it also created extraterritorial impacts on the global nature of the

75. Colchester et al., *supra* note 67.
77. Id.
79. Id. (quoting JACK GOLDSMITH & TIM WU, *WHO CONTROLS THE INTERNET*? (2006)).
82. See generally Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.
Internet. This section will analyze the Directive, *Google v. AEPD*, the GDPR, and the implications of this E.U. ruling worldwide.

**A. The Data Protection Directive of 1995**

The Directive is still the current governing privacy law in the E.U., and provides protection for individuals by restricting the processing of personal data. Although the Directive was made before the advent of the Internet, the Directive's language has been interpreted to apply to the Internet today. This section will analyze the various terms that were crucially defined in order to ultimately establish the right to be forgotten.

Article I of the Directive instructs member states to protect the fundamental rights and freedoms of natural persons. Particularly, states should protect the right to privacy with respect to the processing of personal data, in accordance with the provisions of the Directive. Some key definitions in Article II include the definition of "processing of personal data" and "controller." Processing of personal data is defined as "any operation or set of operations which is performed upon personal data." Examples of "processing of personal data" include "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." Article 2(d) defines "controller" as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of processing of personal data." Additionally, Article 4 defines the applicability of national laws. Particularly relevant is Article (4)(1)(a) of the Directive which states national laws are

---


88. *Id.*

89. *Id.* art. 2.

90. *Id.* art. 2(b).

91. *Id.*

92. *Id.*

applicable when the "processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State."94

The Directive also delineates other specific rights.95 Article 12 discusses the right of access.96 Specifically, 12(b) states the following:

Member states shall guarantee every data subject the right to ob-
tain from the controller ... as appropriate the rectification, erasure
or blocking of data the processing of which does not comply with
the provisions of this Directive, in particular because of incom-
plete or inaccurate nature of the data.97

Similarly, Article 14 contains the data subject’s right to object, stating in 14(a) that in cases referred to in Article 7(e) and 7(f), “Where there is a justifed objection, the processing instigated by the controller may no longer involve those data."98 The Directive recognizes the balancing of the protection of privacy and other fundamental rights such as the freedom of expression.99 However, it makes clear that exceptions to the right to privacy, as governed by the Directive, may only be made in limited circumstances.100

It is important to point out that despite the Directive’s extensive protection of the right to privacy, there is no express right to be forgotten.101 But these definitions discussed above were what the court analyzed to imply the right to be forgotten in the landmark decision discussed in Google v. AEPD.102 This landmark decision, which established the first right to be forgotten on the Internet, is derived from The Directive whose scope was never considered in the online context.103

94. Id. art. 4(1)(a).
95. See generally id.
96. Id. art. 12.
97. Id. art. 12(b).
98. Council Directive 95/46 1995 art. 14; see Council Directive 95/46 1995 art. 7(e)–(f) (Article 7 states that “Member States shall provide that personal data be processed only if: . . . (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller of third party to whom the data are disclosed, or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection under Article 1(1).”).
99. Id. art. 9.
100. Id.
101. See generally id.
102. See generally Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.
103. Id.
B. Establishment of the Right to be Forgotten: Google v. Angencia Espanola de Proteccion de Dato & Mario Costeja González

1. The Facts

On March 5, 2010, Mario Costeja González filed a complaint with the AEPD. The complaint involved La Vanguardia Ediciones SL, a local Spanish newspaper, as well as Google Spain and Google Inc., collectively referred to as Google. Specifically, González was upset about articles that were published in La Vanguardia many years ago, which contained announcements for a real estate auction related to attachment proceedings. All information involved in the articles was true and was a result of González not paying social security debts. González initially requested the following: (1) that La Vanguardia remove or alter pages to remove his personal data; and (2) that Google remove or conceal this personal data so that it no longer appeared in the search results or in the links to La Vanguardia. González contended that this information, though truthful, was no longer relevant because these proceedings had been resolved for a number of years and therefore should be removed.

2. Procedural History

The AEPD ruled that La Vanguardia was legally justified. However, the AEPD also found Google responsible because Google engaged in “data processing” and was subject to the laws of the Directive. The AEPD determined that it had the power to prevent the access and dissemination of data when it compromises “the fundamental right to data protection and the dignity of persons in the broad sense.” Google appealed the decision to the Audiencia Nacional (The National Court). In its order, the National Court stated that the question of whether a search engine is obligated to protect personal data, which a data subject does not want disseminated to third par-

104. Id. ¶ 14.
105. Id.
106. Id.
107. See Google v. AEPD, Case C-131/12 ¶ 15.
108. Id.
109. Id.
110. Id. ¶ 17; Council Directive 95/46 art. 2(b) ("‘processing of personal data’ shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaption, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure or destruction.").
111. Google v. AEPD, Case C-131/12 ¶ 17.
112. Id. ¶ 18.
ties, depends upon the way the Directive is interpreted. The National Court then referred the case to the Court of Justice of the European Union (CJEU). The role of the Advocate General is to write an opinion when the CJEU hears cases involving new law. The Advocate General’s opinions are not binding but are influential in the final decision.

On June 25, 2013, Advocate General Niilo Jääskinen issued his advisory opinion. The Advocate General found that Google was not responsible under the right to privacy and should not be forced to remove links on its search engine. Specifically, the Advocate General held that while Google’s search activities do fit within the definition of “processing,” Google did not meet the definition of “controller” with respect to the source of the material. Overall, the Advocate General’s Opinion expressed the concern that a contrary ruling could have detrimental effects to the freedom of expression. The opinion states that this would entail sacrificing pivotal rights such as freedom of expression and information. However, the CJEU did not agree.

3. Holding

The CJEU found that the intent of the Data Protection Directive of 1995 was to protect the right of privacy to its utmost. This led the Court to imply a new right—the right to be forgotten. The holding of the CJEU focuses on four interpretations of the Directive: (1) that the activities of search engines fit within the definition of “processing of personal data” and that the operator of the search engine also fits within the definition of a “controller”; (2) the activities are considered within the territory of the Member States when there

113. Id. ¶ 19.
114. Id. ¶ 18–20.
116. Id.
117. See generally Opinion of Advocate General Jääkinen, Google v. AEPD and González (June 25, 2013).
118. Id.
119. Id.
120. See id.
121. Id.
122. See generally Google Spain SL v. Agencia Española de Protección de, 2014 E.C.R.
123. Id. ¶ 53.
124. See generally id.
is a branch or subsidiary in a Member State who directs its activities toward
the Member State; (3) in order to comply with the Directive, the search en-
gine is required to remove the requested search results; and (4) the data sub-
ject’s right to privacy overrides the economic interest of the operator of the
search engine, as well as the general public’s interest, in having access to that
information.125 Accordingly, these holdings interpret the Directive’s intent to
mean that the protection of privacy requires that Google remove the
information.126

The CJEU interprets the language of the Directive according to its over-
all intent. For example, the Court states, “in light of the objective of Direc-
tive 95/46 of ensuring effective and complete protection of the fundamental
rights and freedoms of natural persons, and in particular their right to pri-
vacy, with respect to the procession of personal data, [these] words cannot be
interpreted restrictedly.”127 Again the Court states “first of all, it should be
remembered that . . . Directive 95/46 seeks to ensure a high level of protec-
tion of the fundamental rights and freedoms of natural persons, in particular
their right to privacy, with respect to the processing of personal data.”128 The
Court later states that this broad protection is not absolute and is subject to a
balancing of the opposing rights and interests concerned.129 However, there is
little direction on how to implement this balancing test. The only example
given is a data subject who is in the public sphere, causing the interference
with rights to be justified with the general public’s access to the informa-
tion.130 Further, the Court states that information that is deemed to be “inac-
curate . . . inadequate, irrelevant, or excessive with relation to the purposes of
the processing, that are not kept up to date, or that are kept for longer than is
necessary unless required to be kept for historical, statistical, or scientific
purposes” is incompatible with the Directive and warrants a right to be for-
gotten.131 Accordingly, the data subject may request the removal of informa-
tion from the search engine.132 If the search engine or controller does not
grant the request, the data subject may bring suit against the search engine.133

125. Id. ¶ 100.
126. Id.
127. Id. ¶ 53.
128. Google v. AEPD, Case C-131/12 ¶ 66.
129. Id. ¶ 74.
130. Id. ¶ 97.
131. Id. ¶ 92.
132. Id. ¶¶ 77, 92.
133. Id. ¶ 77.
C. The General Date Protection Regulation

Under *Google v. AEPD*, there is not a complete right to be forgotten but rather a right to make information harder to find.\(^{134}\) However, the E.U. is now looking to expand this controversial ruling even farther with the General Data Protection Regulation (GDPR).\(^{135}\) The GDPR would take the place of the Directive and expand the Directive’s scope significantly.\(^{136}\) It would also apply equally to private persons, public officials, and public figures, eliminating the few exceptions that were discussed in *Google v. AEPD*.\(^{137}\) The only exceptions to be included in the GDPR recognize the public’s interest in the exercise of freedom of expression; public health; historical, statistical, and scientific research purposes; and complaints with a legal obligation to retain personal data.\(^{138}\)

The GDPR was proposed in January 2012 and approved by the Civil Liberties, Justice and Home Affairs Committee of the European Parliament.\(^{139}\) The E.U. Parliament approved the GDPR, so these regulations will supersede the Directive when it becomes effective in 2017.\(^{140}\) The E.U. Commission, Parliament, and Council must agree on a final form, but it appears that the E.U. will explicitly recognize the right to be forgotten.\(^{141}\)

---

134. See generally *Google v. AEPD*, Case C-131/12 ¶ 92.

135. See generally GDPR, *supra* note 27.

136. Courtney Bowman, *A Primer on the GDPR: What You Need to Know*, PRIVACY LAW BLOG, http://privacylaw.proskauer.com/2015/12/articles/european-union/a-primer-on-the-gdpr-what-you-need-to-know/ (last visited Sept. 22, 2016) (stating that any company that markets goods or services to E.U. residents may be viewed as a subject to the GDPR, regardless of whether the company is located or uses equipment in the E.U. or not. This provision essentially makes the GDPR a worldwide law).


140. *Id.* at 367.

D. The Implications of the European Union’s Right to Be Forgotten

Many questions still remain with the E.U.’s right to be forgotten. Some of the main points of contention are proper implementation and the alteration of accessible information worldwide. First, the right to be forgotten has created an administrative nightmare for Google. As of March 2015, Google has had to process nearly 218,320 requests for removal of information. Google and other search engines must then evaluate these requests and implement the ambiguous standard as established by the Court. Stefan Kulk, a Dutch researcher, stated, “Google is making decisions that are publicly relevant. As such it is becoming almost like a court or government, but without the fundamental checks on its power.” Is Google being consistent when evaluating these requests? Are there any repercussions for Google if these requests are denied? All of these questions still remain.

Google has released some of the requests that have been made since the E.U.’s decision. These requests put into perspective the decisions that Google has been making throughout this process and illustrate how the right to be forgotten has affected the Internet in the E.U. Some removal decisions are clear-cut while others are more ambiguous. Some of the more clear-cut decisions include the denial of a financial service professional’s request to remove information regarding a past conviction of financial crimes. Equally, a rape victim in Germany requested that a link to an article about the crime be removed; this link was taken down. A less clear-cut decision dealt with a British man who requested that links to an article about a guilty plea be removed. Overall, it appears that ninety-five percent of the removal requests are from ordinary people. Out of the total number of requests, about forty-six percent are removed. While many argue that the legal framework in which Google makes these decisions and alters the Internet in the E.U. is problematic, some see it as a beneficial avenue for individuals.

Dr. Paul Bernal, a lecturer at the University of East Anglia School of Law,

143. Id.
145. Id.
146. Id.
147. Id.
148. Tippman & Powles, supra note 142.
149. Id.
150. See id.
believes that this data proves that the right to be forgotten is a legitimate piece of law. Bernal stated, “if most of the requests are private and personal ones, then it’s a good law for the individual concerned. It seems there is a need for this—and people go for it for genuine reasons.”

Additionally, people should consider the effect that the divided treatment of the right to be forgotten throughout the world has on the World Wide Web. Currently, Google and other search engines must take into account where a user is located to determine what content they can view. Google uses the geo-location of a user to ensure that the E.U.’s citizens cannot see removed material on other countries’ versions of the site. This effectively alters the primary characteristic of the World Wide Web—international accessibility. It also raises the question of the scope of the right to be forgotten. For instance, can a court order for something to be delisted on a worldwide basis rather than just within a certain boundary? This question remains unanswered.

Whether the E.U.’s version of the right to be forgotten will spread to any other countries remains to be seen. Ideally, there would be a worldwide agreement on the necessary actions so that the Internet may once again be a global system. The E.U. Commission’s Vice President directly addressed the United States and this problem by stating, “A message to our American friends. Data Protection rules should apply irrespective of the nationality of the person concerned. Applying different standards to nationals and non-nationals makes no sense in view of the open nature of the internet.” The United States has essentially been asked to adopt the right to be forgotten. But is the right to be forgotten best for the United States?

IV. THE RIGHT TO BE FORGOTTEN IN THE UNITED STATES

Should the United States follow the E.U. and allow individuals the right to control their personal data? Or should we continue to follow our current system, which does not include a right to be forgotten? And if we do accept this right to be forgotten, how vast should it be? These are only a few of the numerous questions that have sparked debate throughout the United States, forcing the United States to weigh the scales of the freedom of expression and the right of privacy.

151. Id.
152. Id.
154. Id. (“In Canada, for instance, the country’s Supreme Court is taking up a case in which a provincial judge ordered Google to delete listing on a worldwide basis—if such a ruling holds, it could embolden judges in other countries to make similar extraterritorial demands.”).
155. Reding, supra note 137.
There is currently a transatlantic split over the right to be forgotten. Historically and presently, the E.U. and the United States hold differing views on the importance of personal privacy.156 This "cultural gap" has created "a battle between two views of freedom—the U.S. belief that free speech trumps everything, and the European view that individuals should have some control over what the world knows about them."157 But is the cultural gap becoming smaller as Americans increasingly value their digital privacy?158 This section will discuss the right to be forgotten in the current U.S. framework by analyzing the following: the current state of the law; the arguments for and against the right to be forgotten; and whether or not the United States will likely adopt the right to be forgotten.

A. Background

Although the United States does not currently recognize the right to be forgotten, it does recognize a right to privacy.159 Cases have discussed the balance between the right to privacy and the freedom of expression. The legislature has also attempted to define privacy protections in a sector specific manner. Determining the boundary between these two dueling rights has progressed over time, yet it has remained unclear as evidenced by case law and legislative history discussed below.

Warren and Brandeis developed the legal right to privacy in a Harvard Law Review article in 1890.160 They defined the right to privacy as an individual's "right of determining ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."161 Warren and Brandeis recognized that the right to privacy is not absolute and must be carved back in certain instances.162 However, since 1890, U.S. courts and the legislature have continued to carve back the right to privacy more than Warren and Brandeis suggested and instead focus on the freedom of expression.

156. See Luckerson, supra note 20.
158. Luckerson, supra note 20 (citing a recent study by the Pew Research Center which found that sixty-eight percent of American Internet users believe U.S. laws don't go far enough to protect individual online privacy).
160. Id.
161. Id.
162. Id.
163. Id.
B. Common Law

The closest case of the right to be forgotten in the United States was in 1931 in Melvin v. Reid.\textsuperscript{164} This case involved Gabrielle Darley Melvin, a former prostitute, who had been tried and acquitted for murder in 1918.\textsuperscript{165} She created a new life for herself, leaving her sordid past behind.\textsuperscript{166} But the defendants, without Melvin’s permission or knowledge, disrupted her new life by releasing a film, Red Kimono, based off Melvin’s past, with the lead character named Gabrielle Darley.\textsuperscript{167} The California Appellate Court concluded that the defendants’ use of her maiden name was “unnecessary and indelicate.”\textsuperscript{168} The court further found that Melvin should have been able to continue in the course of her rehabilitated life without this interference.\textsuperscript{169}

Additionally, a doctrine that seemed to weigh in favor of protecting individuals’ privacy was the “Briscoe doctrine” found in Briscoe v. Reader’s Digest Ass’n.\textsuperscript{170} The plaintiff sued Reader’s Digest for reprinting a story about the plaintiff hijacking a car but failing to mention in the reprint that the crime occurred eleven years earlier.\textsuperscript{171} The court found that Briscoe had a valid cause of action for invasion of his privacy and remanded the case to the trial court for further factual determination.\textsuperscript{172} Although the case pays tribute to the tension between the right of privacy and freedom of expression, the court stated, “the general interest in a unfettered press may at time be outweighed by other great societal interests. As a people we have come to recognize that one of these societal interests is that of protecting an individual’s right to privacy.”\textsuperscript{173}

However, Melvin v. Reid and Briscoe v. Reader’s Digest Ass’n do not represent the current state of privacy laws today.\textsuperscript{174} Many courts have treated Melvin v. Reid negatively\textsuperscript{175} while another case quickly overruled Briscoe v.

\textsuperscript{165} Id. at 286.
\textsuperscript{166} Id.
\textsuperscript{167} Id. at 287.
\textsuperscript{168} Id. at 291.
\textsuperscript{169} Id. at 292.
\textsuperscript{170} See generally Briscoe v. Reader’s Digest Ass’n, 4 Cal.3d 529 (1971).
\textsuperscript{171} Id. at 532.
\textsuperscript{172} Id. at 544.
\textsuperscript{173} Id. at 540–41.
\textsuperscript{174} See id.; see Melvin, 112 Cal. App. at 285.
\textsuperscript{175} Wilan v. Columbia County, 280 F.3d 1160, 1162–63 (7th Cir. 2002) (“the Melvin case, paternalistic in doubting the ability of people of people to give proper rather than excessive weight to a person’s criminal history, is dead.”).
A more accurate depiction of the current U.S. approach to privacy is found in the Second Circuit's opinion in Sidis v. FR Publishing Corp. Although the court acknowledged that other courts recognized a more broad right to privacy such as Melvin v. Reid, the Second Circuit stated: "[W]e are not yet disposed to afford all of the intimate details of private life an absolute immunity from the prying of the press. Everyone will agree that at some point the public interest in obtaining information becomes dominant over the individual's desire for privacy." This effectively ruled against the right to be forgotten.

Since Sidis v. FR Publishing Corp., the United States has generally upheld the free dissemination of information through publication but has not addressed how this relates to the Internet. Currently, courts champion the public interest and the free flow of information. However, the Internet has created a dramatic increase in the amount and accessibility of information. This information is often personal and the record of it does not fade away as with many publications in the past. Although Sidis reflects the general U.S. perspective of freedom of expression, the revolution in information availability creates a new salience to Sidis's holding so many years ago.

C. Current U.S. Privacy Law

The United States does not have a national privacy law but rather a "patchwork system" of various federal and state regulations. In contrast, the E.U.'s right to be forgotten acts as a "blanket" or national law. At the federal level, the Federal Trade Commission (FTC) is the primary enforcer of the various U.S. privacy laws. The FTC uses its authority under the FTC Act to bring various privacy enforcement actions against entities whose information practices have been found to be deceptive or unfair. Besides the

176. Gates v. Discovery Comms., Inc., 101 P.3d 552, 562 (Cal. 2004) (holding that a corporation was not liable for publishing facts obtained from public records).
177. See generally Sidis v. F-R Publ’g Corp., 113 F.2d 806 (2d Cir. 1940).
178. Id. at 809.
180. Id. at 51.
181. Id. at 68.
182. Id.
183. Id. at 69.
185. Id.
FTC, different privacy requirements and laws apply to different sectors and activities. For example, the federal agency handles the interception of communications through the Electronic Communications Privacy Act (ECPA), which is composed of the Wiretap Act, the Stored Communications Act, and the Pen Register Act. Other federal laws pertaining to specific areas include the Fair Credit Reporting Act, the Children’s Online Privacy Protection Act, the Driver’s Privacy Protection Act, and more. The United States continues to increase its amount of privacy laws, but it does so in a categorical way. In 2015, the following federal bills were introduced: the Consumer Privacy Protection Act; the Student Digital Privacy and Parental Rights Act; and the Data Broker Accountability and Transparency Act. These regulations demonstrate the United States’s current “patchwork” system at the federal level.

There are federal laws that are currently in place that deal with personal data but are not as inclusive as the right to be forgotten. The United States looks at the protection of personal data in a categorical approach as it has with other privacy protections. For example, personal financial and health information is strongly protected by the Financial Services Modernization Act and the Heath Insurance Portability Accountability Act. Likewise, the Controlling the Assault of Non-Solicited Pornography and Marketing Act and the Electronic Communications Privacy Act regulate activities that use personal information, such as telemarketing and commercial email. These federal laws are constantly evolving as a reaction to new technologies and the increase in the accessibility and dissemination of personal information.

States have varying laws that also address the collection and use of personal data. Some federal privacy laws preempt state privacy laws, but this is not always the case. Recently, states have begun to develop security breach

187. Id.
188. Id.
189. Id.
190. See generally Jolly, supra note 184.
192. See generally Jay, supra note 186.
193. Id.
194. Jolly, supra note 184.
195. See id.
196. Id.
notification laws.\textsuperscript{197} These laws generally require notification when personal information is disclosed due to a data breach.\textsuperscript{198} Some states take it a step further and require that entities either destroy or render stored personal information unreadable.\textsuperscript{199} Even without a right to be forgotten, state laws allow some individual control over specific categories of their personal information.\textsuperscript{200} For instance, most states allow juvenile criminal records to be expunged.\textsuperscript{201} In California, minors can even request that websites remove posts that they themselves made public.\textsuperscript{202} Other examples include requirements of warrants for email searches and protection of student data.\textsuperscript{203} Further, states have passed laws about the use of drones and data collected by license plate readers.\textsuperscript{204} Although these controls are very specific, they show that the United States is willing to remove information when it is deemed an infringement on rights. But as Michael D. Hintze, chief privacy counsel at Microsoft states, “It can be counterproductive to have multiple states addressing the same issue, especially with online privacy, which can be national or an international issue.”\textsuperscript{205}

Often in the United States, individuals and corporations are successful in removing information that they consider private under current copyright laws.\textsuperscript{206} U.S. copyright laws cover “original works of authorship” including literary works, pictures, sound recordings, and other user-generated content.\textsuperscript{207} Accordingly, “original works of authorship” may not be posted without the permission of its author.\textsuperscript{208} In practice, copyright law is a very useful tool for owners of photos to get the photos or other information taken down because it was posted without the copyright holder’s permission. However, if

\begin{enumerate}
\item\textsuperscript{197} Id.
\item\textsuperscript{198} Id.
\item\textsuperscript{199} Id.
\item\textsuperscript{200} Michael Hiltzik, Fighting for the Right to be Forgotten on the Web, L.A. \textsc{Times} (Nov. 9, 2014), http://www.latimes.com/business/la-fi-hiltzik-20141109-column.html.
\item\textsuperscript{201} Id.
\item\textsuperscript{202} Id.
\item\textsuperscript{204} Id.
\item\textsuperscript{205} Id.
\item\textsuperscript{206} Jeffrey Toobin, The Solace of Oblivion, \textsc{The New Yorker} (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.
\item\textsuperscript{207} 17 U.S.C. § 102(a) (2012).
\item\textsuperscript{208} Toobin, \textit{supra} note 206.
\end{enumerate}
they themselves did not take the picture, they are not the copyright holder and therefore have no removal rights.

For a more personal example of how copyright laws, though helpful, do not provide a complete protection like the right to be forgotten, one need look no further than Nikki Catsouras.\textsuperscript{209} Nikki Catsouras was a California resident who was killed in a car accident.\textsuperscript{210} Graphic photos of the accident and Catsouras’s body were taken at the crash and eventually published on the Internet.\textsuperscript{211} Although the Catsouras family attempted to remove these photos under copyright law, they were unsuccessful.\textsuperscript{212} Because the photos did not belong to them, they had no right to removal.\textsuperscript{213} On the other hand, if California had adopted a right to be forgotten, the Catsouras family would have a right to request the removal of these photos.

Even without a right to be forgotten, the United States has developed a variety of protections that address the disclosure of information, but they are not as far reaching as the E.U.’s laws, which may pose a problem for U.S. citizens in certain instances. Should the United States continue to address privacy problems in this sporadic, reactive manner? Or should the United States adopt a blanket provision like the E.U.? That question garners intense debate throughout the United States and must be addressed.

V. THE DEBATE

With the recent E.U. decision and the general need to reevaluate past common law privacy laws, the topic of potentially adopting the right to be forgotten in the United States has become an ongoing public discussion. As \textit{Time Magazine} stated, the E.U.’s “surprising decision, which Google can’t directly appeal, is either a bold reclamation of privacy rights in the digital era or a mandate to let anyone rewrite history as they please, depending on your perspective.”\textsuperscript{214} Both sides of the debate agree: this ruling presents a real problem. But is it the right solution? The rest of this paper will discuss the arguments for and against adopting the right to be forgotten in the United States. Additionally, it will consider what the legislature or the Supreme Court will do in response to this pressing issue.

\textsuperscript{209} Hiltzik, \textit{supra} note 200.

\textsuperscript{210} Id.

\textsuperscript{211} Id. at 194.

\textsuperscript{212} Id.

\textsuperscript{213} Id.

\textsuperscript{214} Luckerson, \textit{supra} note 20.
A. Arguments for the Right to Be Forgotten in the United States

The main argument behind implementing the right to be forgotten is to allow individuals the ability to control their personal data. This argument has a very strong emotional appeal to people in the United States. To put it into perspective, consider what comes up when you search your name on Google. Maybe it is a positive article about your accomplishments or a link to your company’s website. But what if it includes negative information such as decade-old party pictures, court records, or misleading criminal records? How nice would it be if you could request that Google or Yahoo remove those references? That power is what the right to be forgotten offers.

Some believe that the right to be forgotten is just an in-depth analysis of the balancing between the right to privacy and the freedom of expression. While the balance between privacy and free speech may have once existed, it is now at odds with recent technological changes. In the past, knowledge of the context of the situation often controlled the right to privacy. However, personal information that is on the Internet is frequently taken out of context, which distorts its original meaning. Similarly, old information that was hard to obtain is now hard to escape. Proponents of the right to be forgotten contend that it would restore this balance of personal privacy in our modern environment.

Still others argue that the right to be forgotten is censorship. The rebuttal to the censorship argument is that it is not censorship in the traditional sense, since the individual retains the power to request removal of the data. Beyond that, the information, picture, or Facebook post is not deleted from


\[216.\] Kyle Chayka, Should We Have the Right to Be Forgotten Online?, THE DAILY BEAST (July 14, 2015), http://www.thedailybeast.com/articles/2014/07/15/should-we-have-the-right-to-be-forgotten-online.html.

\[217.\] Id.

\[218.\] The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215.

\[219.\] Id.

\[220.\] Id.

\[221.\] Id.

\[222.\] Id.

\[223.\] Id.

\[224.\] The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215.
the original source. The right to be forgotten is simply making that information harder to find.\textsuperscript{225}

Finally, the right to be forgotten might be better for our society.\textsuperscript{226} With an ever-growing record of our triumphs and past mistakes, the Internet has created the idea that “mistakes are forever.”\textsuperscript{227} Is this what we want? “During the Cold War, we despised totalitarian regimes that keeps a dossier on every citizen, holding compromising information in store for the day that it served to discredit him or her.”\textsuperscript{228} With the right to be forgotten as established by Google v. AEPD, there is no guarantee that you can get the negative information taken down.\textsuperscript{229} It may depend on whether you are a public official or whether the public has a greater interest in knowing this information. Regardless, it gives you the right to request to be forgotten.\textsuperscript{230} If that request is denied, it gives a legal course of action.\textsuperscript{231}

\textbf{B. Arguments Against the Right to Be Forgotten in the United States}

The main word used in the argument against the right to be forgotten is the most threatening word in a free, democratic society: censorship.\textsuperscript{232} The right to be forgotten can be argued to be censorship because it creates a right to be able to force people to “forget what they would otherwise remember . . .”; “it conflicts . . . with the right to remember.”\textsuperscript{233} This information is also true information. Libel, defamation, hate speech, and other hurtful types of speech already have laws prohibiting them.\textsuperscript{234} The right to be forgotten would often result in the suppression of the truth.\textsuperscript{235} One of democracy’s founding principles is the free flow of information, and when we’re talking about a broadly scoped right to be forgotten that’s about altering the historical record or making information that was lawfully public no longer accessible to people, it seems

\textsuperscript{225.} See id.

\textsuperscript{226.} See Marc Randazza, \textit{We Need a ‘Right to be Forgotten’ Online}, CNN (May 15, 2014), http://www.cnn.com/2014/05/14/opinion/randazza-google-right-to-privacy.

\textsuperscript{227.} Id.

\textsuperscript{228.} Id.

\textsuperscript{229.} See generally Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.

\textsuperscript{230.} Id.

\textsuperscript{231.} Id. \textsuperscript{77.}

\textsuperscript{232.} \textit{The U.S. Should Adopt the “Right to be Forgotten” Online}, supra note 215.

\textsuperscript{233.} Id.

\textsuperscript{234.} Id.

\textsuperscript{235.} Id.
impossible] to square that with a fundamental right to access information.236

The United States has found that some information is worth censoring, but personal data on search engines does not meet this high burden.237 The United States censors copyright infringement, sexual abuse of children, and other private sector information.238 But these areas of censorship do not compare to the broad right to be forgotten.

A question remains for those who argue that the right to be forgotten is not censorship but represents a balance between the freedom of expression and the right to privacy. Where do we draw the line? According to the E.U. ruling, a search engine should delete information when that information is deemed inadequate, irrelevant, or excessive.239 As a practical matter, this legal standard is unworkably vague.240 Although many legal standards are vague, the search engines are in charge of implementing this standard and are incentivized to err on the side of taking the requested material down.241 If an individual’s request to take down information is denied, he or she may appeal to a supervisory or judicial court.242 However, if Google removes information that does not meet the standards, there are no legal repercussions currently in place.243

Some experts have stated, “the right to be forgotten is a poor solution to a real problem.”244 The E.U.’s right to be forgotten may be too broad of a ruling to implement in the United States. Additionally, there are many other ways the United States could form its own right to be forgotten. For example, “in America we do not believe in censorship but more speech.”245 So an alternative solution “might be to say that the subject of the search can add a link, a comment, or add a symbol that would click you through to whatever

237. The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215.
238. Id.
240. The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215.
241. Id.
242. See generally Google v. AEPD, Case C-131/12.
243. Id.
244. The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215, at 4.
245. Id. at 9.
you want to say about the link.”246 This would be more along the lines of a right to respond.247 Further, it might be that our society needs to evolve and adapt to this developing record. Past mistakes are not meant to ruin a person’s career aspirations for the rest of his or her life.248 Individuals may simply need to deal with the repercussions of their mistakes that appear on the Internet.249 Regardless of the solution for this real problem, the E.U.’s right to be forgotten is arguably an “extreme solution.”250

C. Will the United States Adopt the Right to Be Forgotten

Despite all the arguments for and against, not many consider whether the United States will adopt a right to be forgotten. The question is whether the right to be forgotten fits within our legal framework in terms of freedom of expression and the right to privacy. The answer is no. No does not mean that the United States will not adopt some sort of protections dealing with an individual’s right to privacy online, however, it does mean that the United States will never develop the same broad right to be forgotten as the E.U.

The United States has had similar problems, which seem to warrant a right to be forgotten. For example, in 2014 there was a celebrity photo hacking incident, which affected Jennifer Aniston, Kate Upton, and Ariana Grande, amongst other celebrities.251 Hackers stole nude photos from their phones and posted them online.252 Even though the United States does not have a right to be forgotten, the celebrities still found legal protection through copyright law, which forced Google to remove the images.253 Although it can be argued that a right to be forgotten would make it easier to have such invasive pictures taken down, it simply does not fit within the United States’ legal framework.254

The E.U.’s right to be forgotten does not reconcile with the United States’ strong commitment to the First Amendment.255 In order to be “cen-

246. Id.
247. Id.
248. See id. at 10.
249. Id. at 44.
250. The U.S. Should Adopt the “Right to be Forgotten” Online, supra note 215, at 44.
252. Id.
253. Id.
254. See id.
255. Luckerson, supra note 20.
sored” the data must pass a high burden, and embarrassing personal data that appears on a search engine does not meet that burden. In the end, free speech trumps privacy in the United States in most instances. But America is not without privacy protections. Although dispersed amongst a variety of federal and state laws, these laws address the few times in which data must be stringently protected. This patchwork system has evolved with the changing technology in the United States, as it will soon evolve to address the continued dispersion of personal data. The United States cannot quickly adapt to the E.U.’s expansive right to be forgotten. To do so would be an overhaul of the United States’s whole free speech and right to privacy system, unnecessarily changing the working system the United States has already implemented.

The E.U.’s right to be forgotten presents one main danger: the fear of expanding privacy into a blanket protection. In an article in Stanford Law Review, Jeffery Rosen states:

> Although . . . depicted . . . as a modest expansion of existing data privacy rights, in fact it represents the biggest threat to free speech on the Internet in the coming decade. The right to be forgotten could make Facebook and Google, for example, liable for up to two percent of their global income if they fail to remove photos that people post of themselves and later regret, even if the photos have been widely distributed already. Unless the right is defined more precisely when it is promulgated over the next year or so, it could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and freedom of expression, leading to a far less open Internet.256

Do American citizens really want Google being the enforcer of our privacy rights? The right to be forgotten suggests that search engines and other websites should be the ones to decide the balance between the right of privacy and freedom of expression. The government has performed this function for the entirety of U.S. history. That structure is not worth changing in order to create a broader right to privacy.

Even though the Supreme Court could hear a lawsuit similar to Google Spain v. AEPD, a decision comparable to the E.U.’s decision would be impossible based on the current state of the law. Unlike the E.U., which could stretch its Directive to allow such a broad definition of privacy, the United States’ privacy laws are narrowly tailored for a specific sector or activity and could never be interpreted to include the right to be forgotten. Equally, “with Congress’s ability to pass new legislation near an all-time low, it’s doubtful sweeping federal change will suddenly come to the front anytime soon.”257

256. Rosen, supra note 56, at 88.

257. Luckerson, supra note 20.
But even if the United States does not adopt a similar right to be forgotten, the E.U. ruling will likely have global implications.\textsuperscript{258} Although Google will only need to delete requested material in countries with the right to be forgotten, "such measures could lead to a decidedly different Internet experience on American shores compared to European ones."\textsuperscript{259} This concept is antithetical to the open Internet.\textsuperscript{260} It marks an end to a truly open Internet by making it two-tiered based on privacy laws. It would take a huge feat, such as an agreed upon law of privacy, to avoid these varying levels of access across the world. At this point in time, such a feat is simply not possible.\textsuperscript{261}

\section*{VI. CONCLUSION}

Varying polls suggest the United States' conflicting reactions to the right to be forgotten. The audience of the Intelligence Squared Debate, discussed throughout much of this paper, had the following opinion: thirty-five percent for the right to be forgotten, fifty-six percent against the right to be forgotten, and nine percent undecided.\textsuperscript{262} Another study conducted by Software Advice, reports that sixty-one percent of Americans believe that the right to be forgotten is necessary.\textsuperscript{263} However, it also reports that sixty-one percent of Americans are still unsure what exactly a right to be forgotten means.\textsuperscript{264} Within the sixty-one percent there is the following breakdown regarding the opinion on the right to remove "irrelevant" information from search results: thirty-nine percent believe that yes, everyone should have this right; fifteen percent believe that yes, but only minors should have this right; and six percent believe that yes, we should have this right, except public figures.\textsuperscript{265} Out of the thirty-nine percent that do not believe that there should be a right to be forgotten, twenty-one percent believe that it is too hard to define relevancy and eighteen percent believe that the information is public record.\textsuperscript{266} These opposing surveys display how this issue has caused a sharp divide in opinions within the United States.

\begin{thebibliography}{9}
\bibitem{258} Id.
\bibitem{259} Id.
\bibitem{260} Id.
\bibitem{261} Id.
\bibitem{262} \textit{The U.S. Should Adopt the “Right to be Forgotten” Online}, supra note 215, at 1.
\bibitem{265} Humphries, \textit{supra} note 263.
\bibitem{266} Id.
\end{thebibliography}
Within the E.U., the right to be forgotten developed from the Directive, a law that was implemented before the Internet as we know it today.267 Yet, the National Court found that the definitions of the Directive meant that there was a right to be forgotten in terms of search engines.268 Further, proposed laws that become effective in 2017 will make this right explicit and even expand the scope of this right.269 But there are still several questions that arise from the current state of E.U. law. For instance: how are Google and other search engines meant to enforce this vague standard; what is the criteria for evaluating requests; and how far does this right to be forgotten apply? These questions are important to consider not only in evaluating the E.U.'s right to be forgotten but also in considering how the right to be forgotten would apply in the United States.

The United States has created a right to privacy over a long period of time and through a patchwork system.270 Essentially, the United States has a reactive system rather than an overarching right to privacy. The right to privacy in the United States deals mostly with the protection of financial information, healthcare information, and some criminal records.271 In some ways, these rights have adapted to the evolution of the Internet. The Internet has created a record of everyone's personal lives that has not been complemented with any personal control over that information. So therein lies the question: should the United States adopt some sort of right to be forgotten?

The Internet is a complicated, growing network and that growth brings this issue to the forefront. This article does not debate whether this is an issue but considers whether the E.U.'s right to be forgotten is the best solution. As stated before, "the right to be forgotten is a poor solution to a very real problem."272 What is a better solution is now the real debate. Soon Congress will have to address this issue, likely dealing with it as it has in the past, through a sector or activity specific law. But there are still several questions that must be addressed, all centering around the following central question: where do you draw the line between freedom of expression and the right to privacy?

As stated by Forbes, "The digital world is forcing us to re-think our constitutional rights, and in essence re-write them for a new era."273 So how will the United States react? Based on U.S. history in privacy law, it seems that the United States will develop a much more narrow form of control over

268. Id. art. 2 (b), (d); Google Spain SL v. Agencia Española de Protección de Datos, 2014 E.C.R.
269. See generally GDPR, supra note 27.
270. See generally Jolly, supra note 184.
271. Id.
272. The U.S. Should Adopt the "Right to be Forgotten" Online, supra note 215, at 4.
273. Maycotte, supra note 264.
a person's Internet record. The E.U.'s right to be forgotten is simply unworkable and overly broad. The United States will have to tailor this right in order to still fit within the U.S. framework which emphasizes the freedom of expression over almost any other right. The United States must be careful with how it answers this worldwide issue because as seen with the E.U., these decisions have global implications.