

The Internet Doesn't Forget: Redefining Privacy through an American Right to be Forgotten

Demi Marks*

What the “Right to be Forgotten” does is it raises the cost for strangers to find out information about you. It doesn’t make it impossible. So, if you turn out to be a famous important person, become a politician, journalists, biographers can dig it out. It just makes it difficult. But that’s the way things work. That’s the way we secure our homes, for example. We don’t make it impossible to break into our house. That would be far too expensive. We put in a lock that will deter most people. It won’t deter people who are extremely interested in getting into our house. That’s—you raise the cost without making something impossible. That’s a way of putting a thumb on the scale for privacy.¹

I. INTRODUCTION

On January 13, 1999, Hae Min Lee was last seen leaving her high school.² On February 9, 1999, her corpse was found in Leakin Park, having been disposed of after strangulation.³ A year later, on February 25, 2000, her ex-boyfriend, Adnan Syed was found guilty of Lee’s murder and sentenced to life in prison.⁴ While these events might seem like old news, the digital age has pushed them back into the limelight. On October 3, 2014, over fifteen years after the murder of Hae Min Lee, *Serial*, a podcast exploring Lee’s murder and Syed’s guilt, was released to the general public.⁵ To date, *Serial* has become the most downloaded podcast ever produced, with over five million subscribers.⁶

* B.A. Tufts University, 2013; J.D., UCLA School of Law, 2016. The author would like to thank Sanford Marks, Barbara Marks, Lorne Schwartz, and Riggins Schwartz for their support during law school. Special thanks are also owed to Professor David R. Ginsburg and Matthew Papa for their invaluable feedback to drafts of this article.

¹ *The U.S. Should Adopt The “Right To Be Forgotten” Online*, INTELLIGENCE SQUARED U.S. (Mar. 12, 2015), <http://www.intelligencesquaredus.org/debates/us-should-adopt-right-be-forgotten-online>.

² *Serial*, CHICAGO PUBLIC RADIO (Oct. 3, 2014).

³ *Id.*

⁴ *Id.*

⁵ *Id.*

⁶ See David Carr, ‘*Serial*,’ *Podcasting’s First Breakout Hit, Sets Stage for More*, N.Y. TIMES, Nov. 23, 2014, http://www.nytimes.com/2014/11/24/business/media/serial-podcasts-first-breakout-hit-sets-stage-for-more.html?_r=0 (“There has been a rabid debate all over the web about the murder and the show, along with parodies on YouTube and recaps on Slate. “*Serial*” has quickly become the most popular podcast in the history of the form.”).

The podcast has done much to advance the case of Syed; however, the other “characters” in the story might not be as excited about the podcast’s success. Asia McClain, a minor character in the story of Lee’s murder who originally testified to having seen Syed in the library and later recanted her statements, will now forever be marred by the “fame” of *Serial*.⁷ If one types “Asia M” into a Google search bar, her full name automatically fills in from the drop-down menu and two full pages of search results yield stories exclusive to her involvement with Lee’s murder.⁸ Similarly, Jay Wilds, a key character in the podcast who is painted in a negative light and considered to be both an unreliable witness and even a possible suspect to Lee’s murder, will now be associated with *Serial* and the murder of Hae Min Lee, even though he did not consent to his full name being used in the podcast and was not even suspected of the crime fifteen years prior.⁹

While the hype surrounding *Serial* may fade with new seasons, the linkage created between these people and the murder told within the podcast will not go away as quickly or as easily. Even if *Serial* comes out with new seasons that yield new search results and trudges up new cases to consider in relation to the search term “Serial,” a search for Asia McClain or Jay Wilds on the Internet will most certainly yield results pertaining to the murder of Hae Min Lee for the rest of their lives.¹⁰ Since the Google algorithm is not chronologically based,¹¹ it will be hard for these people to “escape” their pasts because of the Internet’s “inability to forget.”

⁷ *Serial*, *supra* note 2. See also Madeleine Morgenstern, *Exclusive: Potential Alibi Witness for Convicted Murderer in ‘Serial’ Breaks Silence With New Affidavit*, THE BLAZE (Jan. 20, 2015, 9:01 AM), <http://www.theblaze.com/stories/2015/01/20/exclusive-potential-alibi-witness-for-convicted-murderer-in-serial-breaks-silence-with-new-affidavit>.

⁸ See Morgenstern, *supra* note 7; See, e.g., Tara Fowler, *Serial: Witness Asia McClain Says She Never Recanted Adnan Syed’s Alibi*, PEOPLE (Jan. 20, 2015, 7:00 PM), <http://www.people.com/article/serial-witness-asia-mcclain-says-she-never-recanted>; Ruth Tam, *‘Serial’ Witness Asia McClain Claims Her Testimony Was Suppressed*, PBS SoCAL (Jan. 21, 2015, 12:06 PM), <http://www.pbs.org/newshour/rundown/serial-witness-asia-mcclain-claims-testimony-surpressed>; Nicky Woolf, *Key Witness in Serial Case Asia McClain Cays Prosecutor Suppressed Testimony*, THE GUARDIAN (Jan. 20, 2015, 3:59 PM), <http://www.theguardian.com/tv-and-radio/2015/jan/20/key-witness-adnan-syed-serial-asia-mcclain>.

⁹ See, e.g., Ariana Bacle, *Jay Wilds Talks About How ‘Serial’ Affected His Life*, ENTERTAINMENT WEEKLY (Dec. 31, 2014, 8:09 PM), <http://www.ew.com/article/2014/12/31/jay-wilds-serial-interview-part-3>; Jon Blistein, *‘Serial’ Witness Jay Wilds Opens Up for First Time*, ROLLING STONE (Dec. 30, 2014), <http://www.rollingstone.com/culture/news/serial-witness-jay-opens-first-time-20141230>; Albert Samaha, *Here’s Why Jay Wilds’ New Interview Won’t Necessarily Help Adnan Syed*, BUZZFEED (Jan. 5, 2015, 5:21 PM), <http://www.buzzfeed.com/albertsamaha/heres-why-jay-wilds-new-interview-wont-necessarily-help-adna#mx-0Aprn63G>; Natasha Vargas-Cooper, *Exclusive: Jay, Key Witness From ‘Serial’ Tells His Story For First Time, Part 1*, THE INTERCEPT (Dec. 29, 2014, 12:55 PM), <https://firstlook.org/theintercept/2014/12/29/exclusive-interview-jay-wilds-star-witness-adnan-syed-serial-case-pt-1>.

¹⁰ The magnitude of having five million people subscribe to a podcast and discuss it on the open Internet contributes to the search results. In the unlikely event that Asia McClain or Jay Wilds participate or are associated with something in the future that is surrounded with as much press and discussion, the Hae Min Lee murder results might dwindle down below this newer, equally notorious event. The chances of that happening however, are much smaller than the chances of that not happening, thus creating the dilemma of the Internet’s infinite memory and skewed search algorithm.

¹¹ *Inside Search: Algorithms*, GOOGLE, <http://www.google.com/insidesearch/howsearchworks/algorithms.html> (last visited May 5, 2016) (explaining that Google’s search comprises hundreds of different

In a world where the Internet is so widely used and trusted to formulate opinions about others, what does an Internet persona attached to Asia McClain and Jay Wilds mean for their ability to get jobs and lead a life free from judgment in connection with the Hae Min Lee case? If a case that is over a decade old can be revisited in such detail so as to be considered “newsworthy” again and tarnish the image of those who had been able to distance themselves from the events of their past, where is this line drawn? At what point does the Internet’s memory begin to intrude upon the protection of one’s sense of self? How can one reconcile the American dream of being able to be whoever you want when people can no longer escape their past or change preconceived notions of who they are or what they stand for?

The European Union has confronted these questions by creating a “Right to be Forgotten” (hereinafter “The Right” where applicable).¹² The Right allows individuals to retreat back into privacy by having certain personal data removed and preventing the further dissemination of such data from their Internet persona.¹³ The Right, as presently construed does not overrule all other rights; however, it collides with the interests of the First Amendment. Additionally, as The Right is still in its infancy in the European Union, there are problems surrounding enforcement, censorship, and abuse, which have fueled critics and data aggregators alike to cast aside The Right as unworkable in the United States.¹⁴

While problems persist, the European Union has created a framework that American companies with a presence in Europe must work with or risk losing their operation within the European Union.¹⁵ The Right requires American businesses that operate within the European Union to comply with the law.¹⁶ This has created

factors to arrive at the organization that appears on any given person’s desktop).

¹² European Commission Factsheet on the “Right to be Forgotten” Ruling C-131/12, available at http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf.

¹³ Persona is the person that appears based on an Internet search of a person. *Id.* See also Rolf H. Weber, *The Right to be Forgotten: More Than a Pandora’s Box?*, 2 J. INTELL. PROP., INFO. TECH., & E-COM. L. 120, 120–35 (2011).

¹⁴ See Winston Maxwell, *Right to be Forgotten Can’t be Enforced on the Internet, says European Security Agency*, HOGAN LOVELLS (Nov. 28, 2012), <http://www.hldataprotection.com/2012/11/articles/international-eu-privacy/right-to-be-forgotten-cant-be-enforced-on-the-internet-says-european-security-agency> (“If search sites suppress everything about an individual that they deem “inadequate, irrelevant, no longer relevant, or excessive,” there won’t be much of an Internet left for authorities to regulate.”); Kashmir Hill, *The ‘Right To Be Forgotten’ Is A Nightmare To Enforce*, FORBES (July 24, 2014, 7:11 PM), <http://www.forbes.com/sites/kashmirhill/2014/07/24/the-right-to-be-forgotten-is-a-nightmare-to-enforce> (“The idea that Europe’s regulators would get to determine what information the rest of the world has access to through Google is a hard pill to swallow and would set a nasty precedent when applied to other local censorship by countries around the world.”); Thomas Tamblyn, *EU’s ‘Right To Be Forgotten’ Is Technically Impossible Says Leading Security Expert*, THE HUFFINGTON POST (AUG. 7, 2014, 4:50 PM) http://www.huffingtonpost.co.uk/2014/07/08/google-right-to-be-forgotten-expert_n_5566922.html.

¹⁵ Court of Justice of the European Union Press Release 70/14, Judgment in Case C-131/12 (May 13, 2014) (where the court recognizes that the right must apply beyond the limited scope of a specific jurisdiction), available at <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (last visited May 5, 2016).

¹⁶ *Id.* See generally, Emma Woollacott, *How Europe’s Right to be Forgotten Affects Your Business*, FORBES (June 27, 2014, 9:14 AM) <http://www.forbes.com/sites/emmawoollacott/2014/06/27/>

considerable difficulties for companies such as Google, Yahoo, and Bing, which are in the business of compiling data that they themselves do not necessarily create.¹⁷ Still, as these companies continue to exist on the Internet with growing influence, it is unsurprising that they might be faced with challenges to the status quo, which has existed since the Internet's inception.

This article proposes that the United States adopt its own form of The Right. Part II will look at the current American framework surrounding privacy law, exploring both the history of the current laws and the problems presented by the current system. Part III will look at the European Union's "Right to be Forgotten," examining both case law that has been successful in regards to this new legal development and what The Right encompasses. Finally, Part IV will conclude by proposing an American "Right to be Forgotten," examining a technological solution, a governmentally regulated tiered system of public data and access solution, and a judicial factors test similar to the Digital Millennium Copyright Act (DMCA). Part IV will then look at the benefits and problems created by each solution before recommending that the factors test be adopted as the best solution to the lack of an American "Right to be Forgotten" in the digital age.

II. PRIVACY LAW IN THE UNITED STATES AND CURRENT PROBLEMS CREATED BY THE DIGITAL AGE

The Fourth Amendment governs privacy law and the standard as to whether privacy protection is appropriate in any given situation is governed by a person's "reasonable expectation of privacy."¹⁸ This standard incorporates both whether a person has a subjective expectation of privacy and whether society would recognize an expectation of privacy.¹⁹ Thus, since the Internet has been construed as an open forum, a person's reasonable expectation of privacy on the Internet is limited even though there are few checks and balances as to what is published, how information is disseminated, and who authors the content on the Internet.

For example, it used to be the case that if one wanted to find something out about a person's public record, one had to go to the public courthouse, wait in line, pay a fee, go home, and wait for documents to arrive in one's mailbox weeks later.²⁰ Today, the same inquiry can be solved in a matter of seconds with the click of a mouse.

how-europes-right-to-be-forgotten-affects-your-business; Mark Scott, 'Right to Be Forgotten' Should Apply Worldwide, *E.U. Panel Says*, N.Y. TIMES (Nov. 26, 2014) <http://www.nytimes.com/2014/11/27/technology/right-to-be-forgotten-should-be-extended-beyond-europe-eu-panel-says.html>.

¹⁷ Facebook does have privacy standards in place for users to self-select. Google is the primary site that this new right has targeted because of its prevalence in the European Union and, thus, will be the major subject of this paper.

¹⁸ Orin S. Kerr, *The Fourth Amendment And New Technologies: Constitutional Myths And The Case For Caution*, 102 MICH. L. REV. 801 (2004).

¹⁹ *Id.*

²⁰ See generally, *Public Records on the Internet: The Privacy Dilemma*, Privacy Rights Clearinghouse (Mar. 14, 2016), <https://www.privacyrights.org/ar/onlinepubrecs.htm> (discussing the dangers of the shifting access to public records with the invention of the internet).

A Google search of a name followed by the words “public record” directs you to Intelius,²¹ an information service that allows you to run background checks, reverse phone look-up, and search people all with the click of a button. Although Intelius is a powerful web tool that serves a myriad of useful functions, it (and other sites just like it) serve to facilitate the shifting definition of privacy by expanding the boundaries of what one expects to be in the private sphere and what one expects to be in the public sphere by making personal records so easily accessible.

A. *Seminal Cases in American Privacy Law*

The Red Kimona,²² a film based on real-life prostitution cases, was released to the public in 1925.²³ The film chronicles the early life of Gabrielle Melvin (née Darley) who, when working as a prostitute, was tried for murder and acquitted.²⁴ Melvin went on to assume a normal life after the debauchery of her youth, however after her past was revealed by the film’s contents, she sued, claiming a right to privacy.²⁵ The court, in examining the lack of uniformity in privacy law, came to eight conclusions drawn primarily from Samuel Warren and Louis Brandeis’s 1890 *Harvard Law Review* article that proposed a person’s “right to be left alone” including:

(1) The right of privacy was unknown to the ancient common law; (2) It is an incident of the person and not of property—a tort for which a right of recovery is given in some jurisdictions; (3) It is a purely personal action, and does not survive, but dies with the person; (4) It does not exist where the person has published the matter complained of, or consented thereto; (5) It does not exist where a person has become so prominent that by his very prominence he has dedicated his life to the public, and thereby waived his right to privacy. There can be no privacy in that which is already public; (6) It does not exist in the dissemination of news and news events, nor in the discussion of events of the life of a person in whom the public has a rightful interest, nor where the information would be of public benefit, as in the case of a candidate for public office; (7) The right of privacy can only be violated by printings, writings, pictures, or other permanent publications or reproductions, and not by word of mouth; (8) The right of action accrues when the publication is made for gain or profit. (This, however, is questioned in some cases).²⁶

The *Melvin* court also recognized that one of the major societal objectives is the “rehabilitation of the fallen and the reformation of the criminal.”²⁷ The court exclaimed that, “Where a person has, by his own efforts, rehabilitated himself, we,

²¹ INTELIUS.COM, <http://www.intelius.com> (allowing people to search various forms of public records including criminal records, background checks, and address lookups for free) (last visited May 5, 2016).

²² References of the time reflect that the film existed in two forms, *The Red Kimona* and *The Red Kimono*.

²³ *Melvin v. Reid*, 297 P. 91 (Cal. Ct. App. 1931) [hereinafter cited as “*Melvin*”].

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.* at 92–93. See Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

²⁷ See *Melvin*, 297 P. at 93.

as right-thinking members of society, should permit him to continue in the path of rectitude rather than throw him back into a life of shame or crime.”²⁸ In recognizing these basic principles, the court ruled in favor of the right of privacy, holding that using Melvin’s name in connection with the story was unnecessary and Melvin had a right to pursue and obtain safety and happiness.²⁹ Thus, the court allowed Melvin, through the passage of time and her own actions, to return to a private life.

While *Melvin v. Reid* serves as a landmark case for privacy law in the United States, *Sidis v. F-R Publishing Corp.* limits the right of privacy granted in *Reid*. Sidis, a famous child prodigy in 1910, retreated away from the limelight wanting to avoid the public eye.³⁰ In 1937, however, Sidis was the subject of a biographical cartoon in *The New Yorker* that not only poked fun at Sidis’s past, but also his current state of being.³¹ In ruling in favor of the defendant, the court highlighted the difficulty in weighing the importance of servicing the public’s interest of having access to information against an individual’s want for privacy.³² The court, while being sure not to make a blanket rule, argued that “truthful comments upon dress, speech, habits, and the ordinary aspects of personality”³³ will usually not be such intimate parts of a person as to be protected by the right of privacy.³⁴

In 1971, however, *Briscoe v. Reader’s Digest Association, Inc.*³⁵ held that the publication of facts, even when true, may constitute an invasion of privacy.³⁶ In *Briscoe*, the defendant published an article about carjacking and mentioned the plaintiff who had been arrested for the crime twelve years prior to the publication.³⁷ The court held that “actionable invasion of privacy may occur through the reckless, offensive, injurious publication of true, but not newsworthy, information concerning the criminal past of a rehabilitated convict.”³⁸ Since the plaintiff had reformed and had not been arrested since, the court, similar to the court in *Melvin*,³⁹ did not find that using his name in the publication was necessary to its purpose nor was the public utility of using his name as important as protecting his privacy.

Briscoe distinguished information that deserved First Amendment protection by focusing on the notion of “hot news,” that which would be of immediate public

²⁸ *Id.*

²⁹ *Id.*

³⁰ *Sidis v. F-R Publishing*, 113 F.2d 806 (2d Cir. 1940).

³¹ *Id.* at 807.

³² *Id.*

³³ *Id.* at 809.

³⁴ *Id.*

³⁵ *Briscoe v. Reader’s Digest Ass’n*, 483 P.2d 34 (Cal. 1971) [hereinafter “*Briscoe*”].

³⁶ In 2004, *Gates* effectively overruled *Briscoe* however, the reasoning behind the case supports a right to privacy and thus, is relevant to the discussion here. *Gates* represents a shifting view of privacy law where public access to information trumps personal rights to privacy. See *Gates v. Discovery Communications, Inc.*, 101 P.3d 552 (Cal. 2004) [hereinafter “*Gates*”].

³⁷ See *Briscoe*, 483 P. 2d at 35.

³⁸ *Id.*

³⁹ See *Melvin* 297 P. at 93.

concern.⁴⁰ The court derives a three-factor test for newsworthiness from *Kapellas v. Kofman*⁴¹ that includes the following factors:

[1] The social value of the facts published, [2] the depth of the article's intrusion into ostensibly private affairs, and [3] the extent to which the party voluntarily acceded to a position of public notoriety.⁴²

The court was not over-inclusive in what should and should not be considered private; it found that individuals who are currently being criminally charged should be identified as such as a matter of public concern.⁴³ Thus, the holding in *Briscoe* was limited to events that no longer maintained the same "newsworthiness" as that mentioned above, including situations where legal proceedings have ended, suspects or offenders have been released, and identification of individuals no longer aid in the solving of a case.⁴⁴

Since *Briscoe* was decided in 1971, case law in the area of privacy law has shifted away from favoring a person's right to privacy over the public value of access to information and courts are now more reluctant to find a privacy right sufficient.⁴⁵ Since any household with a computer and access to the Internet can search Google and find out information about another person, the case law trend away from protecting privacy interests represents the shifting notions of privacy. People no longer have a reasonable expectation of privacy in their past careers, faux pas, or anything else that might be published on the World Wide Web. This information is easily searchable, so it becomes harder to rationalize protecting that which is readily available to the general public. Courts have become less inclined to find a right to privacy where the public does not have a reasonable expectation that their information will remain private, especially when balancing First Amendment considerations against this expectation.

B. *Current Problems Surrounding Privacy in the United States*

One of the most elusive problems surrounding privacy law on the Internet is the current algorithm used by search engines to push data to consumers.⁴⁶ Since

⁴⁰ See *Briscoe*, 483 P.2d at 38.

⁴¹ *Kapellas v. Kofman*, 459 P.2d 912, 922 (examining defamation and privacy rights surrounding a publication about minors).

⁴² *Id.*

⁴³ See *Briscoe*, 482 P.2d at 43.

⁴⁴ *Id.*

⁴⁵ See, e.g., *Cox Broad. v. Cohn*, 420 U.S. 469, 496 (1975) ("The rule would invite timidity and self-censorship and very likely lead to the suppression of many items that would otherwise be published and that should be made available to the public"); *The Florida Star v. B.J.F.*, 491 U.S. 524, 532 (1989) ("[I]f a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order"); and *Gates*, *supra* note 36, at 562 ("[A]n invasion of privacy claim based on allegations of harm caused by a media defendant's publication of facts obtained from public official records of a criminal proceeding is barred by the First Amendment to the United States Constitution").

⁴⁶ See generally, *Inside Search: Algorithms*, *supra* note 11. See also *Inside Search: The Knowledge*

sites such as Google do not follow a strictly chronological format, “old” news can appear at the top of a search depending on popularity, recent searches, and a wealth of other factors that reiterate to consumers the notion that the Internet does not forget.⁴⁷

Consider the case of Hugo Guidotti Russo, a plastic surgeon who was sued for an allegedly botched surgery twenty years ago.⁴⁸ Though Guidotti had been acquitted, the second search result yielded by Googling his name was a newspaper article detailing his client’s complaints.⁴⁹ Guidotti shepherded the adoption of The Right in the European Union and now his name is untethered from these reviews that marred his image since the court found them to be irrelevant or no longer relevant to the aims they were published for. While positive reviews and feedback exist to boost the reputation of a doctor in Guidotti’s position, the Google search algorithm does not necessarily place more recent, and arguably more accurate, results at the top of its feed and instead might perpetuate a negative public image.⁵⁰

Since people remain powerless to the search algorithm, people who have been memorialized on the Internet in a negative light sometimes hire companies that push more, not necessarily true, information onto the Internet’s stratosphere to drown out the negative and incorrect statements.⁵¹ Companies such as Reputation.

Graph, Google <http://www.google.com/insidesearch/features/search/knowledge.html> (last visited May 27, 2015) (explaining how web searches are derived from an autofill feature that helps Google narrow your results into its predetermined results, helping a user to click-through and “use the Knowledge Graph to answer questions you never thought to ask and help you discover more”).

⁴⁷ See, e.g., Conor Dougherty, *Google Adds ‘Mobile Friendliness’ to Its Search Criteria*, N.Y. TIMES (Apr. 20, 2015), http://www.nytimes.com/2015/04/21/technology/google-adds-mobile-friendliness-to-its-search-criteria.html?_r=0 (last visited May 5, 2016) (discussing how Google’s algorithm will shift sites down in search results if they are not mobile friendly).

⁴⁸ See Elizabeth Flock, *Should We Have a Right to be Forgotten Online?*, WASH. POST (Apr. 20, 2011, 12:23 PM), http://www.washingtonpost.com/blogs/worldviews/post/should-we-have-a-right-to-be-forgotten-online/2011/04/20/AF2iOPCE_blog.html (last visited May 5, 2016); see also Kashmir Hill, *Plastic Surgeon’s Legal Quest To Facelift Google Search Results*, FORBES (Mar. 7, 2011, 10:20 AM), <http://www.forbes.com/sites/kashmirhill/2011/03/07/plastic-surgeons-legal-quest-to-facelift-google-search-results> (last visited May 5, 2016).

⁴⁹ See Paul Sonne, Max Colchester, & David Roman, *Plastic Surgeon and Net’s Memory Figure in Google Face-Off in Spain*, WALL STREET JOURNAL (Mar. 7, 2011, 12:01 AM), <http://www.wsj.com/articles/SB10001424052748703921504576094130793996412> (last visited May 5, 2016).

⁵⁰ The Internet allows false claims to spread through republishing. Consider the case of Zick Rubin, a lawyer who had, earlier in life, been a respected social psychologist who was declared dead on the site Wikia.com. When Rubin alerted the site of the false statement, the site refused to correct the misstatement because they had sourced the information from a reliable publication. Rubin was defenseless to the Internet’s sourcing dilemma and had to wait for the Internet to rectify the situation on its own without any recourse available to him as the victim. See Zick Rubin, *How the Internet Tried to Kill Me*, N.Y. TIMES, (Mar. 13, 2011), http://www.nytimes.com/2011/03/13/opinion/13rubin.html?_r=0 (last visited May 5, 2016).

⁵¹ This is in line with the traditional approach that the remedy for bad speech is more speech. See, e.g., Cheryl Lock, *Is Online Reputation Management Worth The Money?*, FORBES (July 26, 2013, 11:58 AM), <http://www.forbes.com/sites/learnvest/2013/07/26/is-online-reputation-management-worth-the-money> (last visited May 5, 2016); Claire Prentice, *Online Profile Spring Cleaning*, BBC NEWS (Sept. 24, 2010), <http://www.bbc.com/news/technology-11381037> (last visited May 5, 2016).

com,⁵² BrandYourself,⁵³ and DeleteMe⁵⁴ operate as Internet reputation management firms, hired to inundate the Internet with publications about an individual to distract from damaging content that cannot be removed.⁵⁵ This temporary solution is only creating further problems for the Internet and those who wish to maintain their (and the Internet's) integrity, but remain helpless in the current digital world.

Preference algorithms push information to Internet users; once a user searches for content on a specific person or topic, the links they click on in response to their search terms are pushed higher in search results for that user and other users searching the same terms.⁵⁶ Once a link gains enough clicks and notoriety, it gains traction on the first page of search results and begins to build a person's Internet persona, even if newer, more relevant information comes along that is not necessarily as searched or clicked on.

C. *Current Solutions Surrounding Privacy in the United States*

Problems surrounding privacy protection are not new to America and many regulations exist, both statutory and otherwise, to protect a person's privacy, however, only in given scenarios. For instance, Fair Information Practices⁵⁷ dictate that infor-

⁵² REPUTATION.COM, <http://www.reputation.com> (last visited May 5, 2016) (a website that lets you control your Internet persona by pushing content to overcome negative results, combatting identity theft, and tracking mentions of your name).

⁵³ BRANDYOURSELF.COM, <https://brandyourself.com> (last visited May 5, 2016) (an online site that helps you maximize search results pertaining to your Internet persona).

⁵⁴ DELETEME, <https://www.abine.com/deleteme/landing.php> (last visited May 5, 2016) (an online site that rids the Internet of personal data about you on major sites including your address, phone number, profiles, and other information available to the public).

⁵⁵ Companies are able to do this by increasing the click counts on the information they are publishing, creating articles surrounding a new topic that outnumber articles that their clients do not necessarily want to appear at the top of search engines, and employing a host of other quick fix solutions to trick the Internet into shifting its algorithm to yield more positive results about a person. *See e.g.*, Cheryl Connor, *The Dark Side Of Reputation Management: How It Affects Your Business*, FORBES (May 9, 2013, 1:44 AM), <http://www.forbes.com/sites/cherylconnor/2013/05/09/the-dark-side-of-reputation-management-how-it-affects-your-business> (last visited May 5, 2016); Steve Hehn, *Fixing Your Online Reputation: There's An Industry For That*, NPR (May 29, 2013, 5:49 PM), <http://www.npr.org/blogs/alltechconsidered/2013/05/29/187080236/Online-Reputation> (last visited May 5, 2016).

⁵⁶ *Id.* *See also* Molly Wood, *Sweeping Away a Search History*, N.Y. Times (Apr. 2, 2014), http://www.nytimes.com/2014/04/03/technology/personaltech/sweeping-away-a-search-history.html?_r=0 (last visited May 5, 2016) ("In addition, your search history can create something called a filter bubble. As you build up a history of clicks and queries, Google will start delivering search results tailored to what it thinks you want to see. As a result, your results start to reinforce your worldview or even start to be less accurate, as you see only sites like those you have clicked on before."). *See also* Autocomplete, Google, <https://support.google.com/websearch/answer/106230?hl=en> (last visited May 27, 2015); Danny Sullivan, *How Google Instant's Autocomplete Suggestions Work*, Searchengineland (Apr. 6, 2011 6:27 PM), <http://searchengineland.com/how-google-instant-autocomplete-suggestions-work-62592> (last visited May 5, 2016).

⁵⁷ The Federal Trade Commission created Fair Information Practice Principles to provide guidelines to companies that compile personal information to make sure that the practice provides privacy protection to individuals.

mation that is no longer necessary for the consumer purpose it was provided for must be deleted, a concept called data minimization.⁵⁸ In bankruptcy, credit reporting, and criminal law, a modified “Right to be Forgotten” already exists in line with the basic notion of forgiving and forgetting which remains a fundamental right.⁵⁹ “[T]he U.S. has traditionally understood itself to be a place where individuals could get a ‘second chance.’”⁶⁰ Additionally, some version of record expungement for criminals trying to escape their records exists in thirty states.⁶¹ For juvenile records, most states generally allow one to seal personal records if one meets certain criterion, such as that one is not on probation and an appropriate amount of time has passed since one has committed a crime.⁶² Finally, there are already laws in place including the Children’s Online Privacy Protection Act of 1998, which requires websites and online applications to provide a mechanism for minor users to remove content that they post on the sites (if those sites are directed at or known to be used by minors).⁶³ While all of these efforts currently serve important purposes, even considered together they do not accomplish a right that is narrow enough to tackle the Internet’s ability to never forget the past.

III. EUROPEAN UNION’S “RIGHT TO BE FORGOTTEN”

In the European Union,⁶⁴ a person can unlink their name from websites through The Right.⁶⁵ The Right does not remove the problematic content from the Internet,

⁵⁸ See Justin Brockman, *Europe Revisiting Privacy Law is Opportunity, not Catastrophe*, CTR. FOR DEMOCRACY & TECH. (Nov. 12, 2010), <http://cdt.org/blogs/justinbrookman/europe-revisiting-privacy-laws-opportunity-not-catastrophe> (last visited May 5, 2016) (“The concept of data minimization—including deleting data no longer necessary to achieve a consumer purpose—has been a bedrock concept of Fair Information Practices . . . for years.”).

⁵⁹ Steven C. Bennet, *The “Right to Be Forgotten”: Reconciling EU and US Perspectives*, 30 BERKELEY J. INT’L L., 161, 167–68 (2012); see e.g., Elisabeth Leamy, *Credit Card Companies Forgive Some Debt*, ABC NEWS (Jan. 19, 2009), <http://abcnews.go.com/Business/Economy/story?id=6662160> (last visited Apr. 15, 2016).

⁶⁰ Jean-Francois Blanchette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 THE INFO. SOC’Y 1, 4 (2002).

⁶¹ Jeffrey Toobin, *The Solace of Oblivion*, THE NEW YORKER (Sept. 29, 2014), <http://www.newyorker.com/magazine/2014/09/29/solace-oblivion> (last visited May 5, 2016) (“Back in the day, criminal records kind of faded away over time . . . They existed, but you couldn’t find them. Nothing fades away anymore. I have a client who says he has a harder time finding a job now than he did when he got out of jail, thirty years ago.”).

⁶² National Center for Youth Law, *How to Seal Your Juvenile Records: What Every Juvenile Should Know* (Apr. 7, 2004), <https://www.hitpages.com/doc/4560445935452160/1> (last visited May 5, 2016).

⁶³ Since federal legislation already exists that serves to provide users with the option to “erase” their digital mark from websites, a more expanded version of this principal is at least feasible to consider. See Children’s Online Privacy Protection Act of 1998, PUB.L. NO. 105–277, § 6501 to 6506, 112 Stat. 2681–728 (1998).

⁶⁴ The European Union is a politico-economic union of 28 member states that allows for movement of goods, people, and trade throughout the member states. The federation of member states agrees on certain matters to have common commercial and legal rules.

⁶⁵ Matt Brian, *What you need to know about the ‘right to be forgotten’ on Google*, Engadget (June 2, 2014), <http://www.engadget.com/2014/06/02/right-to-be-forgotten-explainer> (last visited May 27, 2015)

but instead just untethers the algorithm linking a person's name to the content so that it does not come up in search results.⁶⁶ While this, at first glance, might seem like a radical shift away from freedom of expression and towards censorship, on closer examination, the principle operates on a case-by-case basis in line with European conceptions of privacy.⁶⁷

A. *Application of the "Right to be Forgotten"*

Mario Costeja Gonzalez originally began the fight for The Right because a sixteen-year-old notice in a Spanish newspaper's online archives concerning the foreclosure of his house appeared on the first page of search results for his name, shaping his Internet persona.⁶⁸ Since this newspaper article (along with others that had subsequently republished the notice) appeared near the top of Google search results for his name and hurt his chances of getting loans, jobs, and good first impressions, Gonzalez felt that they should be removed by Google because they were no longer relevant and the issue had long been resolved.⁶⁹ Costeja's case was a landmark ruling because it definitively required Google to comply with European Union data privacy laws, expanding the scope of those laws already in place to apply to the Internet age.⁷⁰

("[B]ear in mind that the information will still exist on the websites that published the original information, Google just won't be able to deliver matches to some queries that you enter. That's to say: the information isn't being erased from the web, just made less easily searchable."). See also, Press Release, *supra* note 15.

⁶⁶ Danny Sullivan, *How Google's New "Right To Be Forgotten" Form Works: An Explainer*, SEARCH ENGINE LAND (May 30, 2014, 2:54 AM), <http://searchengineland.com/google-right-to-be-forgotten-form-192837> (last visited May 27, 2015) ("[R]emovals won't pull a URL out of Google worldwide. Instead, if a removal is approved, the URL will be dropped for searches on the associated name from all the EU-specific versions of Google that the company maintains"). So far, The Right only applies to European versions of Google such as Google Germany or Google France and not to general Google.com (the American version of Google). Thus, if someone searches for content in America on Google.com that has been removed from Google.de (Google Germany), it will still be accessible on Google.com but will not be available on Google.fr (Google France).

⁶⁷ *Id.* See also, European Commission, *supra* note 12 ("The Court also clarified, that a case-by-case assessment will be needed. Neither the right to the protection of personal data nor and the right to freedom of expression are absolute rights. A fair balance should be sought between the legitimate interest of Internet users and the person's fundamental rights. Freedom of expression carries with it responsibilities and has limits both in the online and offline world.").

⁶⁸ See Charles Arthur, *Explaining The 'Right to be Forgotten' – The Newest Cultural Shibboleth*, THE GUARDIAN (May 14, 2014, 1:42 PM), <http://www.theguardian.com/technology/2014/may/14/explain-right-to-be-forgotten-the-newest-cultural-shibboleth> (last visited May 5, 2016).

⁶⁹ *Id.*

⁷⁰ Data privacy laws in the European Union lagged behind technological innovation and Costeja's fight helped to bring them into the digital age by making the laws applicable to the world wide web. *Id.* See also David Streitfeld, *European Court Lets Users Erase Records on Web*, N.Y. TIMES, May 13, 2014, at A1, available at <http://www.nytimes.com/2014/05/14/technology/google-should-erase-web-links-to-some-personal-data-europes-highest-court-says.html> (last visited May 5, 2016) ("It raised the possibility that a Google search could become as cheery- and as one-sided – as a Facebook profile or an About.me page.").

Virginia de Cunha, a famous Argentinian pop star, had a different fate when trying her case using The Right. De Cunha, who posed for racy pictures prior to her stardom, sued Yahoo to have them removed and was denied.⁷¹ The case served an important role in litigation surrounding The Right because it clarified the role and responsibilities that Internet providers have while also showing that not every notice filed for takedown is automatically going to be granted.⁷²

B. *Framework in Place for the “Right to be Forgotten”*

In March 2014, the European Parliament enacted The Right.⁷³ Prior to The Right, the European Union had laws in place to protect the privacy interests of individuals including both the Rehabilitation of Offenders Act⁷⁴ and the French *le droit d’oubli*,⁷⁵ so the introduction of The Right was in fact just a small step towards uniformity of a principle that has been in place for years.

The Right allows an individual to file a request with a search engine if one believes content linked to one’s Internet persona in search results is either “inadequate, irrelevant or no longer relevant, or excessive in relation to purpose.”⁷⁶ The Right

⁷¹ Edward L. Carter, *Argentina’s Right to be Forgotten*, 27 EMORY INT’L L. REV. 23 (2013). Though she won her original case, which resulted in a complete blackout of images when “Virginia de Cunha” was searched on the web, she has since subsequently lost on appeal. (“(Judge Barbieri) cited Section 230 of the U.S. Communications Decency Act and a similar provision in the EU’s 2000 Electronic Commerce Directive in reiterating that search engines could not be held responsible. Finally, Barbieri invoked Google’s own Terms of Service, stating that Google was not responsible for content on individual websites, and Google’s compliance with the notice and take-down provisions of the U.S. Digital Millennium Copyright Act”).

⁷² As of April 2015, Google has received over 241,731 removal requests and granted 41.5 percent of them. Some of the leading prior acts motivating removal thus far have been fraud/scam incident removals, violent and or serious crime arrest removals, and child pornography arrest removals. Google, *European Privacy Requests for Search Removals*, GOOGLE TRANSPARENCY REPORT, <https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en> (last visited May 5, 2016) (Google had evaluated 947,868 URLs as of this date).

⁷³ *Id.*

⁷⁴ The Rehabilitation of Offenders Act allows certain criminal convictions to be classified as “spent” after a given period of time and thenceforth not referred to in seeking a job, getting insurance, or in civil proceedings. See *Rehabilitation of Offenders Act 1974: A Nacro Guide*, <https://3bx16p38bchl32s0e12di03h-wpengine.netdna-ssl.com/wp-content/uploads/2014/05/rehabilitation-of-offenders-act-1974-guide.pdf> (2015).

⁷⁵ *Le droit d’oubli* is a modified right to be forgotten that was introduced in France prior to the Rights acceptance throughout the European Union. *Le droit d’oubli*, in combination with The Rehabilitation of Offenders Act, laid the framework for The Right and its application across the European Union. See generally, Richard Easton, *The Right to be Forgotten* (July 5, 2014), <http://www.criminallawandjustice.co.uk/features/Right-Be-Forgotten> (last visited May 5, 2016); see also Shadd Maruna, *Judicial Rehabilitation and the ‘Clean Bill of Health’ in Criminal*, 3 EUROPEAN J. OF PROB. 97, 105 (2011), http://www.ejprob.ro/uploads_ro/725/Conclusion_Courts_of_Redemption.pdf.

⁷⁶ Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM (2012) 11 final (Jan. 11, 2012). See also, Directorate C (*Fundamental Rights and Union Citizenship*) of the European Commission, *Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On “Google Spain And Inc v. Agencia Española*

specifically pertains to search engines because they have opted out of being classified as the media under European data protection law, which gives certain protections and exemptions to journalistic work.⁷⁷ Someone who wants to utilize The Right can, for example, go to Google, fill out a form and list all of the links they want removed from the search.⁷⁸ A review board at Google then considers the case presented and responds; if the links are not taken down, the individual requesting the link removal then has the opportunity to present his or her case to a review board.⁷⁹ Links are not automatically removed once a request to remove is filed; each incident is reviewed on a case-by-case basis, similar to the notice and takedown regime for copyright infringement.⁸⁰

While the European Right system has been criticized as allowing people to present fabricated images of themselves, similar to those on Facebook and other popular social media sites, an important feature of The Right is that the sites are ultimately not taken off of the Internet and are still accessible to the public.⁸¹ For example, if someone were to look for information about a fire that happened thirty years prior, a simple search on the incident could yield any previously published information about the arsonist of the fire. If someone was to search the arsonist's name directly, however, and the arsonist had filed (and been granted) a "Right to be Forgotten," then the information would *not* be yielded through a Google search.⁸² The European Right system, thus, serves as a balancing effort to allow an individual's privacy rights to trump the general public's desire to have unchecked access to information.

De Protección De Datos (Aepd) And Mario Costeja González" C-131/12, ARTICLE 29 DATA PROTECTION WORKING PARTY (Nov. 26, 2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf (last visited May 5, 2016) (detailing factors to be considered when utilizing the inadequate, irrelevant, or no longer relevant standards including whether the result relates to a natural person, whether the subject plays a role in public life or is a public figure, and whether the data subject is a minor amongst a multitude of other factors).

⁷⁷ Journalistic endeavors serve a different function with their main aim being to alert the public, and thus, as such, they qualify for exemptions that search engines, whose main goal is to provide the public with access to a wide range of results without guaranteeing or assuming a purpose, do not. Sullivan, *supra* note 66. See also Arthur, *supra* note 68.

⁷⁸ Sullivan, *supra* note 66. See, e.g., *Search removal request under data protection law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited May 5, 2016) (the Google form for filing a request in Europe).

⁷⁹ *Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited May 5, 2016) (the Google form for filing a request in Europe).

⁸⁰ *Id.*

⁸¹ Arthur, *supra* note 68. See also Streitfeld, *supra* note 70.

⁸² Google is used throughout this paper because it is the dominant search engine throughout the European Union. The Right applies to Yahoo, Bing, and other search engines with equal force.

C. *Problems with Bringing the European “Right to be Forgotten” to the U.S.*

The European Union favors an individual’s right to privacy to a degree that the United States does not.⁸³ While the United States does recognize a limited right to privacy, the current available protections are insufficient for the digital age and ultimately need revamping. While people believe that the right of privacy that existed as of the new millennium is intact, this is not entirely true because of the Internet. Information that used to be considerably hard to obtain can now be accessed with the click of a mouse, via the Internet. Thus, while a case such as *Melvin v. Reid* would not necessarily result in a different outcome, the significance of the ruling would be subdued by the ease of access to information created by the Internet and the shifting public conception of what is private information.⁸⁴

The European Union is typified by a high degree of legislation and judicial involvement in data privacy protection.⁸⁵ The European Union does not require the same principles that are expressed in the American First Amendment, thereby, allowing the E.U. to more easily draw a line between public and private information; in America, the First Amendment serves as a hallmark of freedom and thus, encroaching on this right would be completely counter to American lawmaking and oversight.

Additionally, American commentators fear that The Right is vague, subjective, a means of censorship, prone to abuse, and favors the elite in the European Union.⁸⁶ Other commentators argue that The Right is not fully realized enough for American adoption. The European Union argues that once Google decides to remove a link, they should *not* notify the owner and/or creator of that link that the information has been removed, which would stifle access to information.⁸⁷ Along this line of

⁸³ See Ian Ballon, E-Commerce and Internet Law § 26.01 (2011).

⁸⁴ In the European Union, The Right has clarified the right to privacy in the digital age. Arthur, *supra* note 68 (“What happens when the right to privacy collides with the right to freedom of expression? In the (European court of justice) judges’ view, the answer is fairly clear: the right to privacy wins . . .”).

⁸⁵ See James Gordley, When is the Use of Foreign Law Possible? A Hard Case: The Protection of Privacy in Europe and the United States, 67 LA. L. REV. 1073 (2007); W. Kuan Hon, Christopher Millard & Ian Walden, The Problem of “Personal Data” in Cloud Computing—What Information is Regulated?, 1 INT’L DATA PRIVACY LAW 211, 211–28 (2011).

⁸⁶ The rule is said to favor the elite because of the vast resources available to them, which, in turn, allows them to hire help to patrol Internet personas and file countless takedown requests. See Intelligence Squared Debates, *supra* note 1. See also Jonathan Zittrain, *Don’t Force Google to ‘Forget’*, N.Y. TIMES (May 14, 2014) <http://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html> (last visited May 5, 2016).

⁸⁷ The European Union is arguing that notifying the websites is counter to the purpose of the law and might encourage the websites to come up with workarounds to have their sites appear in search results after they are removed because of The Right rulings. *Id.*; see generally, Sam Schechner, *Google Says It Has the Right to Notify Publishers of ‘Forgotten’ Requests*, WALL ST. J.: DIGITS (July 31, 2014, 12:48 PM), <http://blogs.wsj.com/digits/2014/07/31/google-says-it-has-right-to-notify-publishers-of-requests-to-be-forgotten> (last visited May 5, 2016) (Google argues that notification is essential to the proper balancing of this new right against old standards).

thinking, commentators further argue that the vague, general standards will result in the American population “betraying all the great things the informational revolution has brought us, along with the bad,” because erasing information is not the standard in America.⁸⁸ Currently, the American solution to bad press remains *more* press; instead of fixing the problem directly, the norm in American society has always been to mute the problem by making it less important. The Internet, however, changes the nature of society’s access to information because, even when one publishes more, it does not necessarily become more prevalent than that which already exists and thus, the current means of fixing bad press does not work in the digital age. While the European Union has developed a different attitude towards privacy than the United States, the E.U.’s different approach has generally allowed for the implementation of The Right, whereas American societal values would require a shift in the way false information is rectified.

IV. PROPOSED “RIGHT TO BE FORGOTTEN” SOLUTIONS FOR THE UNITED STATES

While the European framework for The Right has been deemed “a bad solution to a very real problem” by American commentators,⁸⁹ a similar right should exist to protect American citizens’ privacy rights in the digital age. This section will examine three solutions: 1) a technological solution that reformats the way the Internet is organized and places information chronologically in search results, 2) a tiered system of access that creates password protection for different sites so that some information has a higher barrier of entry, and 3) a notice and takedown factors test that applies to websites on a case-by-case basis to determine if the site should be untethered from search results.

A. *Technological Solution*

The simplest solution to the problem created by the Internet as to privacy is to reform the way the current technology operates. As it exists currently, there is not much regulating how search engines cultivate and present data to the public. This lack of search engine regulation, in turn, has created skewed search results with harming effects and could be ameliorated by reforming results into either a chronological format or a password-protected format.

If search engines were presented in a chronological format, “hot news” would presumably appear at the top of the results. For example, as new developments in a given story arise, these updates would continue to push a story into the top of the search results. Chronological order would create a survival-of-the-fittest type system where information that maintains its “newsworthiness” remains accessible, while other data that is no longer as pertinent or relevant to current issues falls further down in the search results. This solution would allow people to recreate themselves and/or

⁸⁸ *Id.*

⁸⁹ *Id.*; see also Streitfeld, *supra* note 70.

retreat to privacy by flushing out old information on a person's life timeline with new events and data. While recentness currently plays a role in the algorithm of popular sites like Google, Yahoo, Bing, Yelp, Facebook, and others, it remains only one of many factors; search engine services are increasingly moving away from chronological formulations to instead include popularity, most viewed, highest rated, and other criteria into a weighted system.⁹⁰

A password protected format would also utilize time to measure relevance; however, this solution would not require sites to completely reformat their current systems in place and instead could archive information and require a password to access information that is older and no longer relevant.⁹¹ An alternative to setting a hard time limit for data shifting to a password-protected site would be to have different types of data disappear to password protected sites at different times. For example, someone who commits a crime, serves time, and then lives a law-abiding life for double the length of punishment could file to have that information moved to a password protected site, which would enable them to rehabilitate and live a life free from judgment.⁹² This system presents problems, however, when trying to formulate how long data that is potentially embarrassing, but not illegal, should remain on the open Internet, or how long data pertaining to arrests where a person is found not guilty or settles a case should remain. Sociologists and psychologists have broken down the life cycle into various stages,⁹³ and these stages could potentially serve as markers for when someone can request for something to be moved to a password-protected site. These stages, however, are more individualized decisions that would require case-by-case review, which would defeat the purpose of having sites automatically shift once time limits have run.

While password-protected sites will no longer be as easily accessible, the sites will not fully disappear. The lack of disappearance poses a similarity to sites, as they currently exist, in the European Union's Right to be Forgotten framework.⁹⁴ While password-protected sites will be untethered from search results, the public will have

⁹⁰ The specifics of how these factors are weighed against each other is not public information and varies from search to search and site to site. Still, it is important to note that a multitude of factors go into the search algorithm to create the results from a search engine query. *See generally*, Inside Search: Algorithms, *supra* note 11.

⁹¹ The problem with this is that older information could still be relevant as part of an ongoing investigation, as important to determining characteristics about a person, or for a vast amount of other reasons. Thus, while setting a hard line (i.e. after five years of a site being unedited, it will become password protected) sounds workable in theory, in practice it would be much harder to implement.

⁹² This time limit is just a suggestion to make an example of how the system could work. Thus, if someone served one year for a misdemeanor, two years after being released from prison, the website chronicling their wrongdoing and prison time would be moved to a password protected site where it would still be available but more heavily guarded. More research would be required to figure out the exact timing of when a person has proven to be law-abiding again and should thus be allowed to file requests for removal.

⁹³ *See, e.g.*, Edward J. Eberle, Human Dignity, Privacy, and Personality in German and American Constitutional Law, 1997 Utah L. Rev. 963 (1997).

⁹⁴ *See Sullivan, supra* note 66.

access to the sites through filed requests. This system will make it harder to find out about peoples' pasts, while still maintaining public interest in freedom of expression, ideas, and the press.

The benefits of this password-protected solution are also negatives. While this system rids the companies, consumers, and government of a lot of the process surrounding hearing each case on an individual basis, it also adds a degree of censorship to the process by removing all information, as opposed to just information that someone has asked to be removed. Problems persist where not all of the information on a given site might be relevant to that information which requires that the site be moved to password protection.⁹⁵ Additionally, deciding who will bear the cost and implementation of this solution remains a problem, as each individual site would be required to play a significant role of setting up a password-protected portal for archived sites, moving sites to this portal once their expiration has been reached, and dealing with the complexities of regulating this technology. Since the shift to the password-protected site will be time-based, deciding when the last significant update to a site occurred will be difficult to regulate because site creators could change small details and claim that the site has been updated and thus does not need to be removed. Enforcement and uniformity of this system would be a major hurdle, and since the time-based expiration pertains to the individual sites and not just search engines, regulatory and oversight problems would make this solution less than ideal.

B. *Tiered System of Public Data*

Similar to the technological solution presented above, a tiered system of public data could be introduced by the government instead of by private companies.⁹⁶ This solution would shift the onus of policing away from private sites and into the government's jurisdiction, which would allow for better management and more uniform terms. The tiered system of public data also does not have to be based on the passage of time and instead could utilize some of the factors of the notice and takedown test below.

For this tiered system to operate differently than the factors test described below (which is based on case-by-case review), the government would be responsible for the initial movement of information from tier one to tier two. Further, the

⁹⁵ An alternative could be that only some portions of the site are moved to another tier and an alert message could appear where the password-protected information was unavailable. There could also be a login screen to every website so that people who have access would not be restricted, but the general public would get a different view of the site (as is the case on Facebook where people who are members and friends with the given person view a different version of their profile than the general public). As I recognize that there are numerous ways this could be implemented, I have chosen to focus on the one presented above.

⁹⁶ A tiered system of public data, in this context, will mean a system where tier 1 is public websites that allow general access to everyone and tier 2 is password-protected data that only allows access, if granted, to specific users.

government could create blanket provisions that classify data based on various factors (e.g., time, type of information, public official status, etc.). For example, specific rules could be set to require that all activity of minors moves to Tier 2 after an individual turns eighteen years old or, alternatively, that all newspaper articles that have not been linked to more current news will be moved to Tier 2 after ten years. The line drawing (similar to the line drawing required for creating time limit expirations for the chronological solution above) that is required for such definitive rules would be especially problematic because of the seriousness of different crimes, the public figure status of different individuals at different times, and the varied societal value derived from different situations, amongst other things.

Alternatively, the government could slow the access to information by not making every piece of information available instantaneously, and instead devise a filter system that classifies the public value into a tiered system prior to dissemination, basically creating a delay for every website being disseminated to the public. This solution, however, would most likely be rejected as a form of censorship, as it would give “big brother” too much power to control information.⁹⁷

A tiered system could facilitate a workable solution, but it creates a lot of work for the government that is not necessarily desired by the general public or helpful in protecting specific privacy interests. Placing the control in the hands of the government, without any prompting from citizens, (as opposed to an individual filing a request similar to the way The Right operates in the European Union) creates vast censorship problems.

C. *Notice and Take Down Factors Test*

The Digital Millennium Copyright Act (DMCA)⁹⁸ operates through a notice and takedown system where copyright owners can file a notice with a website to remove infringing content.⁹⁹ Once reviewed by the site, the site operators can decide if the content is infringing and thereafter remove it. However, the content owners can also file a counter notification if they feel that their content is not infringing. Additionally, content users can either utilize the fair use defense or argue for another applicable reason that may apply and consequently allow the content users to keep the content up.¹⁰⁰ If the parties cannot come to a consensus on the content in question, a court can then decide the matter.¹⁰¹

⁹⁷ This solution is akin to data privacy laws in more developing nations, such as China, for example. In China, access to popular sites such as Facebook, Instagram, Twitter, and others have been blocked for use.

⁹⁸ Digital Millennium Copyright Act of 1998, PUB. L. 105–304, 17 U.S.C. § 512, 112 Stat. 2860 (1998).

⁹⁹ *Id.*

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

The Right in the European Union works in a similar fashion where individuals file a removal request with a search engine.¹⁰² If the site finds the request appropriate, the user's name and likeness are effectively unlinked from the content so that they do not appear when that person is searched.¹⁰³ Thus, the data still remains on the Internet; however, it is untethered from the individual and does not come up in search results for their name.¹⁰⁴ While the factors of the case-by-case analysis should be tweaked to match American laws and customs, this set up provides a more workable solution for dealing with a conception of The Right in the United States.

Under a notice-and-takedown solution, an individual could file a notice with a search engine to unlink their name and likeness from specific information. The site would then perform a balancing test of the following factors: (1) Public figure or public official status; (2) Newsworthiness of the information; (3) Age of the subject when the content in question was created or disseminated versus the age of the subject now; (4) Type of information being deleted; (5) Subsequent arrest, convictions, or acts relating to the information trying to be forgotten; (6) Forgiveness granted in other forms (either by being released from jail, case being decided, etc.); and (7) Public concern and well-being. Each of the foregoing factors will be analyzed below.¹⁰⁵ Because this is a balancing test, none of the above factors are determinative to the outcome, but instead will be weighed equally in any given scenario.

1. **PUBLIC FIGURE OR PUBLIC OFFICIAL STATUS.** The public figure or public official status of an individual is important because of the elevated public concern surrounding these individuals.¹⁰⁶ The bar for public officials or public figures to utilize a Right to be Forgotten must be much higher than for an average citizen, as can be seen in defamation and privacy cases where the Supreme Court recognized the importance of public figure and public official information, whether that information is true or false, to be known.¹⁰⁷ This creates an elevated doctrine of newsworthiness (see below) and stops these individuals from using The Right to hide their pasts from the public.¹⁰⁸ Problems with this

¹⁰² Sullivan, *supra* note 66.

¹⁰³ Brian, *supra* note 65.

¹⁰⁴ *Id.*; see generally Eberle, *supra* note 93.

¹⁰⁵ The multifactor test is a balancing test; however, certain factors are intended to weigh more heavily in the analysis, similar to the Fair Use Test developed by the courts. Where the presence or absence of a factor would make it highly unlikely that information would be taken down if requested, I have made note of the factors' importance in a footnote below.

¹⁰⁶ If someone is a current public figure or public official, it is highly unlikely that his request will be fulfilled. If someone was previously a public official, this factor might weigh against them but will not be as conclusive. If someone files a request for removal and then later decides to run for public office, there will be a high likelihood that the sites asked to be untethered will be reviewed and potentially put back up as they then become matters of public concern and well-being.

¹⁰⁷ See generally *N.Y. Times v. Sullivan*, 376 U.S. 254 (1964) (making it harder for a public figure to win a defamation claim by requiring actual knowledge of falsity or reckless disregard of truth).

¹⁰⁸ *Id.* See also Samuel Gibbs, *Larry Page: 'Right To Be Forgotten' Could Empower Government Repression*, **THE GUARDIAN** (May 30, 2014), <http://www.theguardian.com/technology/2014/may/30/>

system arise if an individual files to have information removed prior to becoming a public figure or public official; however, because these claims originate with a search engine and require a shift in the algorithm of search results, it should similarly be possible to undo or re-tweak the algorithm so as to have information reappear in the instance that an individual becomes a person in the public eye.

2. **NEWSWORTHINESS.** The newsworthiness of a piece of information ties into the notion of “hot news,” where developing and unsolved scenarios (no matter how long they have persisted) continue to be relevant if they are still being investigated and important to matters of public concern.¹⁰⁹ Additionally, the newsworthiness of someone having committed a first degree murder would, for instance, require a higher threshold than a petty theft, because the former remains relevant to the public much longer due to increased public concern, as opposed to the latter.¹¹⁰ Since newsworthiness is a subjective notion, this factor presents problems; however, courts have used this concept before and have been able to circumvent some of the more difficult scenarios posed by this dilemma.¹¹¹
3. **AGE OF THE SUBJECT WHEN ACT IS COMMITTED VERSUS CURRENT AGE.** The age of the subject when the act was committed versus the subject’s current age plays into the American ideal that people should not be held responsible for the debauchery of their youth for eternity. The United States has already enacted protocols, including the Children’s Online Privacy Protection Law, which expunges juvenile records available in most states.¹¹² Additionally, sociologists have emphasized the importance of people being able to rebrand themselves and shed their former skins as they learn and grow, and age plays an important factor in this analysis.¹¹³
4. **TYPE OF INFORMATION BEING UNLINKED.** Depending on how cumbersome the site is, whether the information in question is of a criminal or personal nature, and what kind of file is being disseminated, a removal request would carry different weight based on the type of information being unlinked.¹¹⁴ Any infor-

lary-page-right-to-be-forgotten-government-repression (relating Google’s “power to reject a takedown request if it thinks that the information is in the public interest” to the divide between public figures and ‘everyday’ people).

¹⁰⁹ See *Briscoe*, 483 P. 2d at 38.

¹¹⁰ While newsworthiness is a particularly important factor in considering developing cases and crimes, this factor would play less of a role in the analysis of embarrassing or non-harmful websites as whether or not they are newsworthy is unlikely to apply.

¹¹¹ *Id.* The *Briscoe* case is a perfect example of this type of balancing where old news was found not to be newsworthy any longer. Dissimilarly, *Sidis*, 311 U.S. 711 (1940), found that the new usage for the old news gave it new life. This type of balancing will be formulated by the courts as the test develops and people challenge the rulings of newsworthiness in relation to The Right in the United States.

¹¹² See Children’s Online Privacy Protection Act of 1998, *supra* note 63.

¹¹³ See generally Eberle, *supra* note 93.

¹¹⁴ Consider a gruesome picture of someone being decapitated or a YouTube video of “revenge porn” in contrast to words describing the situation or a newspaper reporting on a car crash or rape case. If the

mation that pertains to criminal activity will be harder to expunge and the more serious the criminal activity, the higher the standard would be in order to be allowed. In contrast, insignificant information that is only accessible to a few and would require extensive work to unlink, such as in the case of password-protected sites and other guarded or buried information, would be less likely to pass muster and be unlinked.

5. **PRIOR ARRESTS, CONVICTIONS, OR ACTS.** If a person who is requesting to utilize The Right has subsequent arrests, convictions, or acts relating to the information they are trying to “erase” from their digital persona, these “bad acts” will weigh against them, as the need for public awareness will trump their right to privacy.¹¹⁵ This factor will be linked to the third factor pertaining to age, as the distance between the two events might make them so separate as to nullify this factor weighing against a person.
6. **FORGIVENESS GRANTED IN OTHER FORMS.** Sometimes settlements are reached, acquittals are decided, judgments are reversed, or people are released from jail; all of which would allow for people to move on and try living a law-abiding existence. These are important occurrences to be considered in deciding if someone should be granted “erasure” of an event in their past, particularly if a conviction is incorrect or a story is incomplete. If forgiveness is granted in another form and the website is not updated or refuses to modify its original posting, a person should be able to make a case for its unlinkage to their name.¹¹⁶
7. **PUBLIC CONCERN AND WELL BEING.** If a website provides information about a person that is of value to society,¹¹⁷ this is a very important consideration to

website is circulating as entertainment before serving some legitimate purpose of informing the public of an event, it is more likely to be erased. *See, e.g.,* Toobin, *supra* note 61 (describing an image of a decapitated girl becoming a meme sensation and her family having no remedies for removal).

¹¹⁵ This factor will weigh heavily against a person and make it highly unlikely that an untethering will be granted as it does not show that the person is living a life free from judgment and rehabilitating.

¹¹⁶ This idea runs counter to the traditional approach of remedying bad speech with more speech because of the way search engines compile their results. The traditional approach does not work on the Internet where older, inaccurate results can gain much more traction than newer, correct ones. Additionally, there are important line drawing considerations that must accompany this factor. For instance, just because someone has been released from jail does not mean that society necessarily completely forgives and forgets their wrongdoing. Further, even if a settlement is reached, that does not mean that there is no public interest in the fact that something happened and the conclusion is unclear. Thus, this factor could not be conclusive on its own as it does not carry the weight of weighing strongly in one’s favor or against it like some of the other factors.

¹¹⁷ Whether something is of value to society is a very subjective standard. Depending on who is deciding the case-by-case analysis of “erasure,” it will be important to weigh all the factors in connection with “value to society” to determine whether there is merit in keeping a website linked to an individual’s persona. If courts are determining the outcome of these case-by-case analyses, it is likely that they will develop examples that demonstrate their understanding of value to society. Some obvious examples include arrests, sexual predators, political remarks and events covered by the news, but these are, by no means, the only examples of information that has is of public concern.

reconcile before untethering that site.¹¹⁸ Public concern seeps into each of the above factors as they must be considered with an eye towards the public and what kind of information should be available to them. Still, if the marginal public benefit that could be gained from knowing something is minimal compared to the elevated personal invasion of privacy or other harms to an individual, public concern cannot always stand in the way of The Right. Public necessity for access to information must be balanced against an individual's rights to come to a proper conclusion regarding the untethering of information from a person's digital footprint.

8. **APPLICATION OF THE FACTORS TEST.** Reconsider the Serial example for both Jay Wilds and Asia McClain, presented at the beginning of this article. If Jay Wilds were to file a request under the factors test to have his Internet persona search results "erased,"¹¹⁹ he would probably succeed in getting his name untethered from the Serial press because his contribution to the story is not new, "hot news;" forgiveness has been granted in another form in that, while he was considered to be a potential suspect at one point, he was never charged with any form of murder or accessory to the murder of Hae Min Lee; he is not a public figure; the age difference is significant (especially in terms of life cycle changes from youth to adulthood); and his involvement in the murder is not of public concern because of his innocence.¹²⁰

Dissimilarly, however, Asia McClain would have a harder time unlinking herself from the murder of Hae Min Lee and the Serial podcast. After the podcast was released in 2014, McClain continued her involvement in the investigation by recanting any of her previous statements and giving new testimony in support of Adnan Syed.¹²¹ Since McClain has participated at different points in her life cycle and contributed "hot news" elements that can help Syed's current appeals process, McClain's request would probably not be granted at this time.¹²² If, however, she were to file this request ten years from now and the subsequent trials have been resolved and her role in them is no longer a matter of public concern, McClain could then reapply for removal. In this way, this system provides the proper check and balance system to the Internet's infinite memory through a fluid, changing notice and takedown procedure.¹²³

¹¹⁸ As public concern and well-being are the most important justifications for keeping all websites up and not creating a right to be forgotten in America, this factor will weigh very heavily in any untethering analysis if this test is adopted. Where there is a justifiable reason for alerting the public to information for their well-being, a site is less likely to be "erased" from an individual's online persona.

¹¹⁹ This refers to the results that come up when one searches for "Jay Wilds."

¹²⁰ See *Serial*, *supra* note 2. See also Vargas-Cooper, *supra* note 9; Samaha, *supra* note 9; Blistein, *supra* note 9; and Baclé *supra* note 9.

¹²¹ *Id.* See also Tam *supra* note 8; Fowler *supra* note 8; Woolf *supra* note 8.

¹²² *Id.*

¹²³ This test can be applied to numerous other scenarios. For example, if a child molester applies for "erasure" of links pertaining to their child molestation, they will be unsuccessful. If a politician wants his collegiate newspaper article in support of his opposing party's views removed, he too will probably

The factors test is the most balanced of the solutions provided; however, it still creates administrative problems, both in the creation of a committee to review these cases and handle the paperwork associated with these requests, and also for the burdens created for the government if these cases are appealed. Additionally problematic is that factors tests in general must maintain a degree of vagueness, but the test articulated in this article aims to fix some of these vagueness problems present in *The Right in the European Union* by giving more concrete characteristics to consider and providing a system that is not equally weighted towards each factor analysis.¹²⁴ Additionally, the test still remains highly subjective and, since the deciders of whether to police or not are private corporations, namely Google, Yahoo, and other search engines, the system remains imperfect.¹²⁵

V. CONCLUSION

In the end, neither *The Right in the European Union* nor the current privacy framework in American law and policy are perfect solutions to the problems created in a digital age. An American conception of *The Right*, however, would be a small step in the right direction of adjusting law and policy to keep up with our rapidly expanding digital age.¹²⁶ “We have reached a critical moment. Control over our personal data has been all but lost online: lost to corporations, to governments; lost to

be unsuccessful. If, though, a child molester wants a fifteen-year-old article about his house being foreclosed untethered, he will probably be able to have this done so long as there are no more recent charges relating to foreclosures or bankruptcy and he is not running for public office or serving as a public official. Similarly, if after serving a term in the Senate, a politician retires from public service and then wants the article removed, he will be able to reapply and this public official status will not weigh against him if he is no longer serving in that capacity or planning to in the future (if however, he does decide to run, there will be a system in place that reexamines candidate’s erasures to see if they should be republished on the Internet because of public concern and well-being).

¹²⁴ The system also does, in a very slight way, favor the wealthy, as it maintains information on the open Internet but makes the process of finding it more difficult and therefore, more timely and expensive, but it does not make it impossible for anyone no matter their wealth to have the same opportunities.

¹²⁵ *The Right* is currently enforced by a committee of Google employees and most decisions are ultimately left in the hands of one Google employee as to whether something should be “erased” or not. This is problematic because it puts the public in hands of private companies (who are often motivated by money and business over altruistic goals) and there is no oversight of this. An unlikely solution to this problem could be that a highly specialized task force convenes comprised of representatives from all search engines who have over a specific number of unique users, government officials, and individuals specialized in privacy, sociology, and psychology. These individuals could determine the take down requests and then all search engines would be notified of the decision and have to comply or appeal on an individual basis. This would help quash some of the excess work created by each search engine being required to create their own task force, while also making the judgments less subjective and prone to bias and convenience (e.g., where a search engine approves the request so that they do not have to deal with a tedious appeals process).

¹²⁶ Gordon L. Crovitz, *Google Speaks Truth to Power*, WALL ST. J. (Oct. 24, 2011), <http://www.wsj.com/articles/SB10001424052970204618704576645353164833940> (last visited May 5, 2016) (“High tech runs three times faster than normal businesses. And the government runs three times slower than normal businesses. So we have a nine-times gap.”).

each other. How can we, as individuals, be empowered by the huge benefits of digital connectivity and global information flows, yet still retain some personal control over the way our identities are represented and traded online?¹²⁷ Our digital personas now exist without locks, and, just as it is dangerous to leave our home and our belongings open to intrusion with no protection, so it is unwise to leave our digital footprints unregulated and unchangeable.

¹²⁷ Julia Powles & Enrique Chaparro, *How Google Determined Our Right to be Forgotten*, THE GUARDIAN (Feb. 15, 2015), <http://www.theguardian.com/technology/2015/feb/18/the-right-be-forgotten-google-search> (last visited May 5, 2016).