Gone But Not Forgotten: Recognizing the Right to Be Forgotten in the U.S. to Lessen the Impacts of Data Breaches

ASHLEY STENNING*

TABLE OF CONTENTS

* © 2016 Ashley Stenning. J.D. 2017 candidate, University of San Diego School of Law.

INTRODUCTION

In July 2015, Ashley Madison suffered a large and highly publicized data breach.[1] Data breaches occur regularly and have far reaching consequences because of the amount of personal information being stored online.[2] Technological progress and globalization has made many aspects of daily life more efficient, and, because of this, the Internet has become a place where people communicate and share information. However, in exchange for the efficiency of the Internet, users sacrifice some aspects of their privacy.

With numerous social media websites and applications ("apps") available, users have more platforms to broadcast their personal information. It is no longer a time when information is only stored in people's memories: individuals leave bits of their personal information all over the Internet where it remains stored forever. An embarrassment may no longer end at banter between friends, but instead may live forever online. It is not uncommon for some individuals to publish their lives online without thinking of the consequences.

The majority of users of social media and other websites likely have not read the companies' often lengthy privacy statements and are, therefore, likely not aware of which rights they are giving up with respect to the storage and use of their personal data.[3] Most terms and conditions on Internet sites are completely one-sided and lean in the website's favor, whether this is legal or not.[4] Even individuals who do not partake in social media give third parties access to their personal information by visiting websites, booking online travel, or even opening a bank account, where they essentially leave a digital footprint. Furthermore, individuals, whether they are aware of it or not, permit some websites to disclose their personal information to third parties.[5] Technology has vastly changed how individuals interact and has increased the amount of personal information available to the public.

The following example illustrates the amount of user information websites store. In 2012, an Austrian law student, Max Schrems, requested Facebook

---

1. *See infra* Part I.A.
2. *See generally infra* Part I (discussing data breaches and the globally-recognized "right to be forgotten").
3. *See, e.g.*, *Facebook Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy/ (last visited Jan. 21, 2016).
4. *See, e.g.*, Brian Powers, *Ashley Madison's Online Terms and Conditions May Leave it Legally Undressed*, FORBES (Oct. 22, 2015, 11:40 am), http://www.forbes.com/sites/beltway/2015/10/22/ashley-madisons-online-terms-and-conditions-may-leave-it-legally-undressed/.
5. *See, e.g.*, *Facebook Data Policy*, *supra* note 3. "We work with third party companies who help us provide and improve our Services or who use advertising or related products, which makes it possible to operate our companies and provide free services to people around the world." *Id.*

to release all of its stored information pertaining to him.[6] Facebook complied, and the law student received 1,222 pages of data the company had stored.[7] The retained personal data included event responses,[8] locations, IP login addresses, photos, messages, posts people made on his profile page, removed friends, and virtually every interaction he ever had while using Facebook.[9] After receiving this log of personal information stored by Facebook, Schrems filed 22 complaints against Facebook in Ireland.[10]

Although Facebook's data policy has become more transparent since the law student began his fight against the social media maven,[11] Facebook still retains a plethora of information on its users until the user either deletes his or her account or Facebook decides it "no longer need[s] the data to provide products and services."[12] As such, simply deleting content from Facebook does not necessarily mean the information is no longer catalogued and stored.

With the ever-increasing use of the web, privacy issues are an ongoing concern, and data breaches are becoming more commonplace.[13] The increase in data breaches and privacy concerns raise the inherent question of whether individuals should have the right to remove their information from websites. In light of increasing data breaches, users should not have to worry as much about their personal information getting leaked, especially if the personal data no longer serves any purpose to the website. Removing

---

6. *See* Craig Timberg, *Facebook Privacy Targeted by Austrian Law Student*, THE WASHINGTON POST (Oct. 19, 2012), http://www.washingtonpost.com/business/economy/facebook-privacy-targeted-by-austrian-law-student/2012/10/19/45a38efc-e70c-11e1-936a-b801f1abab19_story.html.

7. *See id.*

8. An event response is how a user responds to an event invitation over Facebook by selecting interested, going, or ignore.

9. *See Data Pool*, EUROPE VERSUS FACEBOOK, http://europe-v-facebook.org/msb2.pdf (last visited Jan. 21, 2016) (providing all data gathered by Facebook regarding user Max Schrems).

10. *See Objectives*, EUROPE VERSUS FACEBOOK, http://europe-v-facebook.org/EN/Objectives/objectives.html (last visited Jan. 21, 2016) (defining Facebook user Max Schrems' purpose for the website).

11. *See* Timberg, *supra* note 6*; see also* Alexis Kleinman, *Facebook Just Made a Big Change to Privacy Settings*, HUFFINGTON POST (May 22, 2014, 10:12 am), http://www.huffingtonpost.com/2014/05/22/ facebook-privacy-settings_n_5372109.html; *see also Updating Our Terms and Policies*, FACEBOOK, https://www.facebook.com/about/terms-updates (last visited Jan 22, 2016).

12. *See Facebook Data Policy*, *supra* note 3.

13. *See* Robert Jett III & Peter Sloan, *Once More Unto the Breach: Why and How to Be Ready for A Data Breach*, 33 ACC DOCKET 36, 38 (2015).

one's information from a website's database underlies the highly debated "right to be forgotten."[14] The European Union recognizes the right to be forgotten, which gives individuals the right to have their personal data removed from online sources, but the United States has not yet recognized it.[15] As society changes, so must the laws. As Samuel Warren and Louis Brandeis stated in *The Right to Privacy*, "[p]olitical, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society."[16]

This Comment will explore the right to be forgotten, how it is recognized in the European Union, and the trend toward the existence of such a right in the United States. Additionally, this comment will discuss how the right to be forgotten could lessen the impact data breaches have on individuals through the lens of the Ashley Madison hack. Lastly, this comment will discuss how, if the United States narrowed the scope of the European Union's concept of the right to be forgotten to fit into the United States' view of privacy and the First Amendment, the impact of data breaches would decrease.

Part I will discuss the origins of the right to be forgotten and its developments and use in the European Union. It will also discuss potential developments both in the United States and around the globe. Part II will discuss data breaches in general, give background on the recent Ashley Madison data breach, and analyze the wide-reaching effects the data breach had on individuals and the company. Part III will introduce how a right to be forgotten could prevent the negative and wide-reaching effects of data breaches. Part IV will consider how to bridge the gap between the differing privacy ideals in the EU and the United States. Lastly, Part V will propose how the right to be forgotten can be altered to fit American values and the American legal framework, and will suggest both legislative and non-legislative ways the right to be forgotten could exist in the United States.

I. DATA BREACHES

Data breaches are a growing concern as personal information is increasingly stored and shared online. A data breach is "a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed,

14. *See, e.g.*, *Debate: Should the U.S. Adopt the 'Right to be Forgotten' Online?*, NAT'L PUBLIC RADIO (Aug. 18, 2015), http://www.npr.org/2015/03/18/393643901/debate-should-the-u-s-adopt-the-right-to-be-forgotten-online.

15. *See* Michael L. Rustad & Sanna Kulevska, *Reconceptualizing the Right to be Forgotten to Enable Transatlantic Data Flow*, 28 HARV. J. L. & TECH. 349, 353 (2015).

16. Samuel Warren & Louis D. Brandeis, *The Right To Privacy*, 4 HARV. L. REV. 193, 193 (1890).

stolen or used by an individual unauthorized to do so."[17] With thousands of breaches occurring each year, nearly every industry is at risk.[18] Data breaches are extremely costly for companies, averaging $217 per compromised record of U.S. data breaches.[19] Data breaches have become more common for many companies, and it is no longer the notion that a breach may occur, but rather *when* a breach will occur.[20] Data breaches are widespread across the globe with many notable high-profile breaches including Home Depot,[21] Sony,[22] Medicentre,[23] and, one of the most recent and highly controversial, Ashley Madison.

A. Ashley Madison Breach

Ashley Madison, owned by Avid Life Media ("ALM"), is a website for adults looking to have extramarital affairs with the tagline: "Life is short. Have an affair."[24] As of January 2016, the Ashley Madison website had over 43 million users.[25]

In July of 2015, a group of hackers, known as "The Impact Team," gained access to Ashley Madison's secured systems and stole large caches of data from the site, including user data, which had the potential to affect over 30 million users.[26] The Impact Team posted a manifesto stating that it decided to publish the stolen information in protest of ALM charging

17. ADMINISTRATION FOR CHILDREN AND FAMILIES, U.S. DEP'T OF HEALTH & HUMAN SERVS., Log No. ACYF-CB-IM-15-04, Information Memorandum (July 1, 2015), *available at* http://www.acf.hhs.gov/sites/default/files/cb/im1504.pdf (last visited Jan. 22, 2015).

18. Jett III & Sloan, *supra* note 13, at 38.

19. *Id.* at 39.

20. *Id.* at 38.

21. Melvin Backman, *Home Depot: 56 Million Cards Exposed in* Breach, CNN: MONEY (Sept. 18, 2014, 5:56 PM), http://money.cnn.com/2014/09/18/technology/security/home-depot-hack/.

22. James Cook, *Sony Hackers Have Over 100 Terabytes of Documents. Only Released 200 Gigabytes So Far*, BUSINESS INSIDER: TECH INSIDER (Dec. 16, 2014, 2:19 PM), http://www.businessinsider.com/the-sony-hackers-still-have-a-massive-amount-of-data-that-hasnt-been-leaked-yet-2014-12.

23. Marianne Kolbasuk McGee, *Breach Among Largest Ever in Canada*, DATA BREACH TODAY (Jan. 23, 2014), http://www.databreachtoday.com/breach-among-largest-ever-in-canada-a-6422.

24. ASHLEY MADISON, https://www.ashleymadison.com (last visited Jan. 22, 2016).

25. *Id.*

26. Brian Krebs, *Online Cheating Site AshleyMadison Hacked*, KREBS ON SECURITY (July 19, 2015, 11:40), http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/.

users $19 for a "full delete," which is a "removal of site usage history and personally identifiable information from the site."[27] The Impact Team alleged the "full delete" was ineffective because users' purchase details were not erased, such as a user's real name and address, information that, according to the hackers, users specifically wanted deleted.[28] The Impact Team's manifesto claimed that the deletion for money scheme "netted ALM $1.7mm in revenue in 2014" and was a "complete lie."[29] The hackers asked for ALM to take down Ashley Madison and Established Men, another ALM dating site, or they would release the stolen information including "customer records, profiles with all the customers' secret sexual fantasies, nude pictures, and conversations and matching credit card transactions, real names and addresses, and employee documents and emails."[30]

In August 2015, after ALM disregarded The Impact Team's threats, the hackers posted the stolen data, including personal data on users that paid for their information to be deleted,[31] and made it accessible to the public.[32] Websites that published the data allowed users to be searched by username.[33] The data breach had far reaching effects, including lawsuits, suicides, public shame, blackmail, and the potential for users' names to be on the list that did not actually make the profile or use the site.[34] This was possible because users were able to create an Ashley Madison account without having to verify their e-mail, which meant that anyone could sign up with someone else's e-mail address.[35] Those individuals were still compromised in the breach.[36] Soon after the release of information, ALM offered a $500,000 CAD reward for information about the hackers that could lead to their arrest.[37]

---

27. *Id.*
28. *Id.*
29. *Id.*
30. *Id.*
31. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/; *see also* Sutts Strosberg LLP, *Ashley Madison Privacy Breach*, https://www.strosbergco.com/class-actions/ashleymadison/ (last visited Jan. 22, 2015).
32. *See* Zetter, supra note 32.
33. *See Ashley Madison Privacy Breach*, *supra* note 31.
34. *See, e.g.,* Kristin V. Brown, *Scared, Dead, Relieved: How the Ashley Madison Hack Changed Its Victims' Lives*, FUSION (Dec. 9, 2015, 2:14 PM), http://fusion.net/story/242502/ashley-madison-hack-aftermath/.
35. Doug Bolton, *Ashley Madison Leak: The Personal Details of 32 Million Users Might Not All Be Genuine*, INDEPENDENT (Aug. 19, 2015), http://www.independent.co.uk/life-style/gadgets-and-tech/news/ashley-madison-hack-live-email-verification-10461653.html.
36. *Id.*
37. Rob Gillies, *Ashley Madison Hack Under Investigation*, ASSOCIATED PRESS (Aug. 24, 2015), http://www.usnews.com/news/business/articles/2015/08/24/cheating-site-ashley-madison-offers-reward-for-info-on-hack.

Currently, two Canadian law firms have filed a $578 million class action lawsuit against both ALM and Ashley Madison on behalf of Canadian residents who used Ashley Madison.[38] The law firms stated that "[t]he action seeks damages for breach of contract, breach of consumer protection statutes, negligence, intrusion upon seclusion, breach of privacy and publicity given to private life for Ashley Madison customers whose personal information was publicly disclosed on August 18, 2015."[39] At least four more suits have been filed in the United States claiming ALM and Ashley Madison are in "breach of contract, engaged in negligence in protecting customer data and violated various state privacy laws" and that "the companies knew their networks were insecure."[40] Essentially, the lawsuits claim that not enough steps were taken by Ashley Madison and ALM to keep Ashley Madison users' information and identities secured.[41] One suit filed alludes to emotional distress and describes the release of information as a "nightmare," and states that the "revelation of personal and financial information 'is bound to have catastrophic effects on the lives of the website's users,'"[42] thus illustrating the devastating emotional impact of data breaches.

Interestingly, Ashley Madison's terms and conditions state Ashley Madison can change its terms and conditions at anytime, and it is the user's responsibility to periodically check for these changes.[43] The statement goes on to say that a user's continued use of the site after any changes will mean that the user accepts the change.[44] Consequently, users of Ashley Madison may have been accepting terms and conditions without having any knowledge of them or any subsequent changes.

Even if it is difficult to sympathize with people being caught using Ashley Madison, it is easy to sympathize with spouses of users who publicly discovered their spouse used the adultery site. Undoubtedly, the breach

38. Tanya Basu, *Ashley Madison Faces $578 Million Class Action Lawsuit*, TIME (Aug. 23, 2015), http://time.com/4007374/ashley-madison-578-million-lawsuit-canada/.

39. *See Ashley Madison Privacy Breach*, *supra* note 31.

40. Kim Zetter, *Ashley Madison Hit With $500 Million in Lawsuits*, WIRED (Aug. 25, 2015), http://www.wired.com/2015/08/ashley-madison-hit-500-million-lawsuits/.

41. Chris Isidore, *Ashley Madison Sued by Anonymous Clients*, CNN: MONEY (Aug. 25, 2015), http://money.cnn.com/2015/08/25/news/companies/ashley-madison-lawsuits/.

42. *Id.*

43. *Ashley Madison Terms & Conditions*, ASHLEY MADISON, https://www.ashleymadison.com/app/public/tandc.p?c=1 (last visited Jan. 21, 2016).

44. *Id.*

has put large strains on many marriages.[45] It is a much easier case to sympathize with people who had their information on the site without actually ever signing up for it. The Impact Team reminded the public that the Ashley Madison site is littered with "thousands of fake female profiles,"[46] and with no verification process, some users identified in the breach may not have actually signed up for the site.[47]

The data breach has also paved the way for extortion. Bryce Evans, Staff Superintendent of the Toronto Police, explained that "the ripple effect of the impact team's actions has and will continue to have a long term social and economic impacts, and they have already sparked spin-offs of crimes and further victimization," and stated that there have already been two unconfirmed suicides that are associated to the Ashley Madison data breach.[48] Users received threats that their "dirt" would be disclosed to their family, friends, and employers if they were not given money.[49] On top of trying to extort money from users, scammers sent out e-mails offering links to the leaked information,[50] as well as malware-infested e-mails to users offering links to "scrub" their information.[51] Once the malicious software was installed, the criminals could gain access to anything stored on the computer, such as passwords and bank account information, which not only impacted users, but also those interested in the hack.[52] The Ashley Madison data breach opened many doors for other hackers and scammers to further hurt the individuals affected by the breach.[53] Surprisingly, after the breach, the number of Ashley Madison users did not decline,[54] suggesting a multitude of attitudes, including the sentiment that the benefits of social media outweigh the possible effects of a data breach.

---

45. Jose Pagliery, *The Ashley Madison Hack Ruined My Life*, CNN: MONEY (Aug. 21, 2015), http://money.cnn.com/2015/08/21/technology/ashley-madison-ruined-lives/.

46. *See* Zetter, *supra* note 31.

47. Bolton, *supra* note 35.

48. Brian Krebs, *Ashley Madison: 500K Bounty for Hackers*, KREBS ON SECURITY (Aug. 24, 2015), http://krebsonsecurity.com/2015/08/ashleymadison-500k-bounty-for-hackers/.

49. Katie Rogers, *After Ashley Madison Hack, Police in Toronto Detail a Global Fallout*, N.Y. TIMES (Aug. 24, 2015), http://www.nytimes.com/2015/08/25/technology/after-ashley-madison-hack-police-in-toronto-detail-a-global-fallout.html.

50. Aimee Picchi, *Ashley Madison Hack Leads to Scams, Extortion*, CBS NEWS (Aug. 24, 2015), http://www.cbsnews.com/news/scams-extortion-attempts-arising-from-ashley-madison-hack/.

51. Jonah Bromwich, *Ashley Madison Users Face Threats of Blackmail and Identity Theft*, N.Y. TIMES (Aug. 27, 2015), http://www.nytimes.com/2015/08/28/technology/ashley-madison-users-face-threats-of-blackmail-and-identity-theft.html.

52. *Id.*

53. *Id.*

54. ASHLEY MADISON, *supra* note 24.

Noel Biderman, the chief executive officer of ALM, resigned shortly after the hackers released the stolen data.[55] Days later, ALM released a statement claiming that "[media] reports predicting the imminent demise of Ashley Madison are greatly exaggerated."[56] The company also claimed "hundreds of thousands of new users signed up for the Ashley Madison platform,"[57] demonstrating the company's continued growth since the hack. This growth may also demonstrate how important social media is to individuals, even in light of the risk of data breaches.

The effects of data breaches are far-reaching, as exemplified by the Ashley Madison hack. Potential effects that have an economical cost for data breaches include market consequences, penalties, and various consumer impacts.[58] The right to be forgotten could lessen such impacts by allowing users to have more control over the ability to manage their personal information on the web; however, there still continues to be a debate over whether the U.S. should establish a right to be forgotten.

II. BACKGROUND ON THE RIGHT TO BE FORGOTTEN

The right to be forgotten is a fairly new concept that recognizes an individual's right to privacy in a growing digital age, which encompasses an individual's right to control and remove personal information held and stored on the web.[59] The right to be forgotten has been proposed in a data reform and will come into effect in Europe at the beginning of 2018, two years after the European Parliament and Council formally adopt the final texts.[60] However, the European Court of Justice did not wait for the data reform to become effective before recognizing the right to be forgotten,

55. Press Release, *Statement from Avid Life Media – August 28, 2015*, ASHLEY MADISON (Aug. 28, 2015), http://media.ashleymadison.com/statement-from-avid-life-media-august-28-2015/ (last visited Jan. 22, 2016).

56. Press Release, *Statement From Avid Life Media, Monday, August 31, 2015*, PR NEWSWIRE (August 31, 2015, 7:00 PM), http://www.prnewswire.com/news-releases/statement-from-avid-life-media-monday-august-31-2015-300135089.html.

57. *Id.*

58. *See* Alessandro Acquisti et al., *Is There a Cost to Privacy Breaches? An Event Study*, in ICIS 2006 Proceedings 1563, 1573 (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-friedman-telang-privacy-breaches.pdf.

59. *See* Allyson Haynes Stuart, *Google Search Results: Buried if Not Forgotten*, 15 N.C. J.L. & Tech. 463, 465 (2014).

60. *See* Press Release, EUROPEAN COMM'N, *Agreement on Commission's EU Data Protection Reform Will Boost Digital Single Market* (Dec. 15, 2015), http://europa.eu/rapid/press-release_IP-15-6321_en.htm (last visited Jan. 26, 2016).

giving European citizens the right to permanently remove their personal data from the web.[61] The right aims to find a balance between an individual's right to privacy and society's right to know.[62] The right to be forgotten is a concept that is recognized in the European Union but not in the United States, albeit there is a slight drift towards the recognition of such a right in the United States.[63] The First Amendment creates a hurdle in applying the right to be forgotten in the U.S. as it exists in the EU.[64]

A. The Right to Be Forgotten in the European Union

1. 1995 Data Protection Directive

The European Union ("EU") has been at the forefront of data protection, viewing privacy as a fundamental human right.[65] With its adoption of the Data Protection Directive 95/46/EC ("the 1995 Directive") in 1995, the European Union has solidified its progressive stance in protecting an individual's right to privacy.[66]

Although comprehensive, the 1995 Directive was written at a time where many of the online services in use today, such as social media sites, did not exist, so modernization to the 1995 Directive is needed.[67] Furthermore, there are inconsistencies in how each Member State has implemented the laws set out in the 1995 Directive, which have led to complexities, legal uncertainty, and administrative costs.[68] As such, the European Parliament and Council have agreed on a data protection reform.[69]

---

61. *See infra* note 83 and accompanying text.
62. *See infra* note 88 and accompanying text.
63. *See infra* Part II.B.
64. *See infra* Part IV.A.
65. *See 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)*, at 1, COM (2012) 11 final (Jan. 25, 2012) [hereinafter GDPR]; *see also* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 461–62 (2000).
66. *See generally* Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, 1995 O.J. (L 281), 23.11.1995 P. 0031 – 0051, http://eur-lex.europa.eu/legalcontent/en/ALL/?uri=CELEX:31995L0046 (last visited Jan. 23, 2016) [hereinafter Directive 95/46/EC] (regulating personal data processing in the EU).
67. European Commission Press Release, Questions and Answers - Data Protection Reform (Dec. 21, 2015), http://europa.eu/rapid/pressrelease_MEMO-15-6385_en.htm.
68. *Id.*
69. *Id.*

a. The Reform

In 2012, the European Commission ("Commission") proposed a comprehensive reform to the 1995 Directive, known as the General Data Protection Regulation ("GDPR"), to strengthen online privacy rights.[70] One of the objectives of the GDPR is to give control back to citizens over their personal data.[71] The need for the GDPR solidifies the dramatic increase of data sharing and collecting.[72] The European Commission recognizes in the GDPR that "[t]echnology allows both private companies and public authorities to make use of personal data on an unprecedented scale in order to pursue their activities."[73] As technology expands, so must the law. Article 17 of the GDPR contains the notion of the right to be forgotten.[74]

When the reform is effective, the right to be forgotten under the GDPR will give the data subject[75] the right to have the data controller[76] remove

---

70. GDPR, *supra* note 65, at 19.
71. *Id.* at 1.
72. *See id.*
73. *Id.*
74. *Id.* art. 17.

> The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies: (a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; (b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data; (c) the data subject objects to the processing of personal data pursuant to Article 19; (d) the processing of the data does not comply with this Regulation for other reasons.

Id.

75. *Id.* art. 4.

> A data subject is an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, psychological, genetic, mental, economic, cultural or social identity of that person.

Id.

76. *Id.*

> Article 2 of the directive 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by Union law or Member State law, the

their personal data and the discontinuance of further dissemination.[77] The right to be forgotten would be strengthened under the GDPR by requiring the data controller to prove that they need to keep the data, rather than the data subject having to prove that keeping their personal data is unnecessary.[78] The GDPR will give individuals easier access to their data.[79]

2. Google Spain v. AEPD

The European Court of Justice ("CJEU") did not wait for reform to come into effect before recognizing the right to be forgotten itself in a landmark case against Google Inc. ("Google") in 2014, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González* (Google Spain v. AEPD or "Google Spain").[80] The case was initiated by a Spanish man's request to delist search results that linked to news stories about his unpaid debts, dating back to 1998.[81] The case called for an interpretation of the Directive in relation to an individual's protection in the processing of personal data.[82] The Court declared Google a data controller,[83] giving data subjects the right to request Google to remove their personal data.[84] The Court also solidified the right to be forgotten by ruling that a data subject has the right to ask for information to no longer be made public as long as it is not outweighed by both "the economic interest of the operator of the search engine" and "the interest of the general public in having access to that information upon a search relating to the data subject's name."[85] The Court determined that delisting is available

---

controller or the specific criteria for his nomination may be designated by Union law or by Member State law.

Id.

77. *Id.* art. 17.

> Where the controller . . . has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

Id.

78. *See generally id.*

79. *See id.* art. 14.

80. *See* Case C-131/12, Google Spain SL. v. Agencia Española de Protección de Datos (AEPD), ECLI:EU:C:2014:317 (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN [hereinafter *Google Spain*].

81. *Id.*

82. *Id.* at 2.

83. *Id.* ¶ 41.

84. *See* GDPR, *supra* note 65, art. 17.

85. *Google Spain*, *supra* note 80, ¶ 99.

for links that "appear to be inadequate, irrelevant or no longer relevant or excessive in the light of the time that had elapsed."[86]

The result of the *Google Spain* ruling has triggered Google to now have a form for individuals to complete in order to delink personal information for its EU domain extensions.[87] After the request is made to Google to remove a link to certain information, Google will "balance the privacy rights of the individual with the public's interest to know and the right to distribute information."[88] Google states that:

> When evaluating your request, we will look at whether the results include outdated information about you, as well as whether there's a public interest in the information — for example, we may decline to remove certain information about financial scams, professional malpractice, criminal convictions, or public conduct of government officials.[89]

Google will fulfill a request "deemed inadequate, irrelevant, no longer relevant or excessive, and not in the public interest" by "delist[ing] it from search results for that individual's name from all European versions of Google Search" (emphasis omitted).[90] The right to be forgotten is essentially weighed against whether society should have the right to access the information. In order to fulfill a request, Google requires a digital copy of some form of identification.[91] Google has claimed that in just over a year, it has received over 250,000 requests to delist links to over 1,000,000 different web pages.[92] However, even if Google removes a link on its EU domains, it may still remain on Google's other domains, such as the U.S. Google extension, which has created controversy with the French data protection regulator, which will be discussed below.[93]

---

86. *Id.* ¶ 93.
87. *Search removal request under data protection law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Jan. 21, 2016) [hereinafter GOOGLE LEGAL HELP].
88. *Id.*
89. *Id.*
90. Peter Fleischer, *Implementing a European, not global, right to be forgotten*, GOOGLE: GOOGLE EUROPE BLOG (July 30, 2015), http://googlepolicyeurope.blogspot.be/2015/07/implementing-european-not-global-right.html [hereinafter GOOGLE EUROPE BLOG].
91. GOOGLE LEGAL HELP, *supra* note 87.
92. GOOGLE EUROPE BLOG, *supra* note 90.
93. *Id.*

3. *Commission Nationale de L'informatique et des Libertés ("CNIL")*

The ability of individuals to find content delisted from EU Google domains by using other Google domains where the information still remains listed diminishes the effectiveness of the *Google Spain v. AEPD* ruling.[94] In May of 2015, the Commission Nationale de L'informatique et des Libertés ("CNIL"), France's data protection regulator, publicly ordered Google to apply delisting requests to "all extensions of the search engine."[95] The CNIL considered the CJEU's decision and concluded that, in order for the decision to be effective, the requested links should be removed on all Google extensions.[96] Once the CNIL put Google on notice, it gave Google fifteen days to comply and delist the requests for removal on all versions of Google.[97]

In July of 2015, Google responded by rejecting the CNIL's order to apply the delisting to all Google extensions by asking the CNIL to withdraw its formal notice.[98] Through a public announcement, Google argued that complying with the order "risks serious chilling effects on the web."[99] Google referenced that the right to be forgotten, while recognized and enforced in the EU, is not the law globally, and thus, cannot be applied globally.[100] Furthermore, Google continued to illustrate the chilling effect by stating that "the Internet would only be as free as the world's least free place" if it were to follow the CNIL's order.[101] Google reached this conclusion by offering that content that is deemed illegal in one country could exercise the removal of such content on all Google extensions.[102] Google requested the CNIL to withdraw its formal notice with its main argument being "that it would impede the public's right to information and would be a form of

---

94. *CNIL Orders Google To Apply Delisting on All Domain Names of the Search Engine*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (June 12, 2015), https://www.cnil.fr/fr/node/15790.

95. *Id.*

96. *Id.*

97. *Id.*

98. GOOGLE EUROPE BLOG, *supra* note 90.

99. *Id.*

100. *Id.*

101. *Id.*

102. *Id.*

> While the right to be forgotten may now be the law in Europe, it is not the law globally. Moreover, there are innumerable examples around the world where content that is declared illegal under the laws of one country, would be deemed legal in others: Thailand criminalizes some speech that is critical of its King, Turkey criminalizes some speech that is critical of Ataturk, and Russia outlaws some speech that is deemed to be "gay propaganda."

Id.

censorship."[103]

In July of 2015, Google accidentally released statistical data on the delinking requests it had received.[104] The data shed light on the fact that "95% of Google privacy requests are from citizens seeking to protect personal and private information—not criminals, politicians or public figures."[105] Virtually, all requests to delist links are for private, personal information, and, of these requests; only about half are granted with about one third being rejected and the other portion still pending.[106] Less than 1% of the total amounts of requests granted were for a "serious crime," "public figure," "political," or "child protection."[107] Google could have granted those requests "because they concern[ed] victims, incidental witnesses, spent convictions, or the private lives of public persons."[108] Because the data sourced from Google does not specify whether the source's requests were made by the source's subject or by a third party, there is the potential that the requests could have been made by a victim or witness.[109]

Google maintains its own Transparency Report that documents Government requests to remove content and Europeans privacy requests for delisting, among other reports.[110] Google's Transparency Report shows that the United States government makes more requests on average than any EU state,[111] demonstrating the idea of a right to be forgotten is not lost on the United States.

By September of 2015, the President of the CNIL rejected "Google's informal appeal against the formal notice requesting it to apply delisting on all of the search engine's domain names" by putting Google on notice,

---

103. *Right to Delisting: Google Informal Appeal Rejected*, COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS (Sept. 14, 2015), http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/ [hereinafter CNIL Appeal Rejected].

104. Sylvia Tippmann & Julia Powles, *Google Accidently Reveals Data on 'Right to be Forgotten' Requests*, THE GUARDIAN (July 14, 2015), http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests. The Guardian found hidden data in source code in a transparency report released by Google that indicated where most requests for delinking came from.

105. *Id.*

106. *Id.*

107. *Id.*

108. *Id.*

109. *Id.*

110. *Google Transparency Report*, GOOGLE, https://www.google.com/transparency report/ (last visited Jan. 21, 2016).

111. *Download the Data*, GOOGLE, http://www.google.com/transparencyreport/removals/government/data/?hl=en (last visited Jan. 21, 2016).

which requires Google to comply with the CNIL's request or risk sanctions.[112] The CNIL rejected Google's appeal for numerous reasons, among them being: that being able to use another Google extension to find information that was delisted from another extension would circumvent the right to be forgotten, impeding the right's efficiency; that the information would not fully be deleted as it would still be available on the source website or another search engine—the delisting only impedes the results from appearing from a search of an individual's name; and that the "right is not absolute" as it is weighed against the public's right to information.[113] This conflict demonstrates the inconsistent laws and views between the EU and the United States.

B. Trends Towards a Right to Be Forgotten in the United States

The United States currently does not recognize such a "right to be forgotten" as the CJEU does.[114] However, the United States has witnessed developments towards adopting such a right for decades. To start, in the 1931 case of *Melvin v. Reid*, in which a former prostitute acquitted of murder wished to sue a producer of a film that depicted her previous life she no longer wanted to be associated with, the California Court of Appeals recognized:

> One of the major objectives of society as it is now constituted, and of the administration of our penal system, is the rehabilitation of the fallen and the reformation of the criminal. Under these theories of sociology it is our object to lift up and sustain the unfortunate rather than tear him down. Where a person has by his own efforts rehabilitated himself, we, 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. Even the thief on the cross was permitted to repent during the hours of his final agony.[115]

The right to be forgotten falls in line with idea that individuals should be given a second chance without being reminded of their previous actions.

In 1890, Warren and Brandeis' article, *The Right to Privacy*, was published.[116] The authors advocated for the recognition of a right to privacy noticing that numerous areas of law seemingly already realized this right.[117] Warren and Brandeis saw the right to privacy as a "right to be let alone," and recognized the right's fluidity throughout time.[118] The roots of the right to be forgotten can be seen further throughout changes to American law.

---

112. CNIL Appeal Rejected, *supra* note 103.
113. *Id.*
114. Garcia v. Google, Inc., 786 F.3d 733, 745 (9th Cir. 2015).
115. Melvin v. Reid, 112 Cal. App. 285, 292 (Dist. Ct. App. 1931).
116. Warren & Brandeis, *supra* note 16.
117. *See generally id.*
118. *Id.* at 195.

At the beginning of 2015, following the EU's acknowledgment of a right to be forgotten, California enacted its own version of the right, applying it only to minors.[119] The law gives minors the right to remove, or request to remove, information and content that minor users posted.[120] It does not, however, apply to content that minors were given compensation for, or content that a third party posted.[121] Minor users only have the right to removal for information they themselves have submitted.

Revenge porn, the non-consensual distribution of sexually explicit images,[122] is also consistent with the idea of a right to be forgotten. The California legislature has enacted a revenge porn statute, making the intentional distribution of pornographic material of another person illegal.[123] The original version of the law, which California first enacted in 2014, did not recognize self-taken photographs.[124] Since 2015, the legislature has updated the law to apply to both self-taken images or images taken by another person where the photographer understands that the image is meant to remain private or has knowledge, or should have knowledge, that the sharing of the image "will cause serious emotional distress."[125] The recognition that individuals have the right to privacy in a digital age further paves the way for a right to be forgotten in the United States.

Furthermore, following in the footsteps of the EU, Congress introduced the Consumer Privacy Bill of Rights Act of 2015 ("Consumer Privacy

---

119. CAL. BUS. & PROF. CODE §§ 22580–81 (Deering 2016) (defining "Minor" as a natural person under 18 years of age who resides in the state).

120. *Id.* § 22581(a)(1).

121. *See id*. § 22581(b)(2), (b)(5).

122. *See* Sarah Bloom, Note, *No Vengeance for 'Revenge Porn' Victims: Unraveling Why This Latest Female-Centric, Intimate-Partner Offense is Still Legal, and Why We Should Criminalize It*, 42 FORDHAM URB. L.J. 233, 237 (2014).

123. *See* CAL. PEN. CODE § 647 (J)(4)(A) (Deering 2016):

> Any person who intentionally distributes the image of the intimate body part or parts of another identifiable person, or an image of the person depicted engaged in an act of sexual intercourse, sodomy, oral copulation, sexual penetration, or an image of masturbation by the person depicted or in which the person depicted participates, under circumstances in which the persons agree or understand that the image shall remain private, the person distributing the image knows or should know that distribution of the image will cause serious emotional distress, and the person depicted suffers that distress.

Id.

124. *See* Emily Poole, Comment, *Fighting Back Against Non-Consensual Pornography*, 49 U.S.F. L. REV. 181, 209 (2015).

125. CAL. PEN. CODE § 647 (4)(A) (Deering 2016).

Bill").[126] The proposed bill aims to "establish baseline protections for individual privacy in the commercial arena."[127] The bill applies to Covered Entities, which Congress has defined as "a person that collects, creates, processes, retains, uses, or discloses personal data."[128] The bill calls for the following main principals:

(1) Transparency: Individuals have a right to understandable, accurate, and reasonable notice of a covered entities privacy and security practices.[129]

(2) Individual Control: Individual's shall be given reasonable means to control how their personal data is processed.[130]

(3) Respect for Context: Covered entities shall only process personal data in ways reasonable to the context in which the individual provided such data.[131]

(4) Focused Collection and Responsible Use: Individuals' personal data may only be collected, retained, and used ways that are reasonable to the context of provided information.[132]

(5) Security: risks to the privacy of personal data shall be identified and safeguarded against by the covered entity.[133]

(6) Access and Accuracy: individuals have the right to reasonable access their personal data retained by the covered entity, and the ability to dispute and resolve the accuracy of the information.[134]

(7) Accountability: covered entities are to take measures to ensure compliance with the Consumer Privacy Bill.[135]

Congress acknowledges that American citizens value their privacy, and that laws must keep up with the evolution of technology.[136] The bill does not expressly state a right to be forgotten; however, under the principle of Individual Control, individuals are given the right to withdraw their consent for data retention, and in response, the Covered Entity is to timely remove the personal data associated with the withdrawal of consent.[137] Although

126. Consumer Privacy Protection Act of 2015, S. 1158, 114th Cong. (2015). An identical bill exists in the House of Representatives. Consumer Privacy Protection Act of 2015, H.R. 2977, 114th Cong. (2015) [hereinafter Consumer Privacy Bill].
127. *Id.* at 1.
128. *Id.* § 4(b).
129. *Id.* § 101.
130. *Id.* § 102.
131. *Id.* § 103.
132. *Id.* § 104.
133. *Id.* § 105.
134. *Id.* § 106.
135. *Id.* § 107.
136. *Id.* § 3.
137. *See id.* § 102(c)(1).

not yet enacted or perfected,[138] the Consumer Privacy Bill exemplifies that privacy rights and a right to be forgotten are not outside the scope of American law.

In 2013, Congress introduced the Application Privacy, Protection, and Security Act ("APPS Act"), with the aim to "provide for greater transparency in and user control over the treatment of data collected by mobile applications and to enhance the security of such data."[139] The APPS Act would require the developer of a mobile application[140] to provide users with notice pertaining to how the application will collect, use, store, and share personal data and obtain consent from the user to such terms before the application collects personal data from the user.[141] Further, the developer of a mobile application would have to provide its application users with a means to notify the developer of their intent to stop using the application and to withdraw consent to any further collection of personal data.[142] The APPS Act would give users the option to request the developer to delete any stored personal data collected from the application, or request the developer "to refrain from any further use or sharing of such data."[143] This Act shows Congress' openness towards adopting the right to be forgotten, and towards giving users more control over their personal data in the United States.

Although the United States does not recognize a right to be forgotten in the same sense as the EU, the United States has still afforded its citizens rights that relate to the right to be forgotten, which demonstrates the value afforded to privacy in the U.S.

1. The Right To Be Forgotten Around the Globe

The EU is not the only jurisdiction to legally recognize a right to be forgotten. Similar rights have been extended in other countries, and some

138. Natasha Singer, *White House Proposes Broad Consumer Data Privacy Bill*, N.Y. TIMES, Feb. 27, 2015, http://www.nytimes.com/2015/02/28/business/white-house-proposes-broad-consumer-data-privacy-bill.html?_r=0.

139. *See generally* Application Privacy, Protection, and Security Act of 2013, H.R. 1913, 113th Cong. (as proposed, May 9, 2013). Reintroduced February 10, 2016, and has been assigned to a congressional committee. *See generally* Application Privacy, Protection, and Security Act of 2016, H. R. 4517, 114th Cong. (as proposed, Feb. 10, 2016).

140. H.R. 1913 § 8 (A mobile application is a software program that "runs on the operating system of mobile device" and "collects data from a user.").

141. *Id.* § 2.

142. *Id.*

143. *Id.*

countries are looking into taking similar steps towards recognizing such a right.

For example, Argentine courts have referenced the idea of the right to be forgotten in the case of *Da Cunha v. Yahoo and Google*.[144] The plaintiff, Virginia Da Cunha, was a dancer, singer, actress, and model from Argentina.[145] Da Cunha, who posted personal photographs on her Twitter and Facebook accounts, found out that Google and Yahoo search results linked her photographs and names to websites that were of a sexual nature.[146] She claimed the erotic websites were doing this without her consent and it was damaging to her career.[147] The trial court concluded that Da Cunha's right to control her images was violated and it ordered Google and Yahoo to pay moral damages to Da Cunha and delete Da Cunha's photographs from search results relating to sexual content.[148] The Appeals court reversed the lower court's decision and ruled in favor of Google and Yahoo, holding that search engines could not be held accountable for the content others decide to post on their own websites.[149] However, one judge still defended that individuals should possess the right to be forgotten, but as search engines, Google and Yahoo could not be held liable for their search results.[150] Although the case was ultimately reversed, the Argentine court still recognized that an individual's right to be forgotten exists.

More countries have afforded their citizens a right to be forgotten, and some are still making efforts towards recognizing such a right. As previously discussed, Google did not want to apply the EU's right to be forgotten globally by allowing information to be delisted from all Google extensions. The *Google v. AEPD* case influenced not only California's recognition of a minor's right to be forgotten, but it also influenced the adoption of such policies in many countries spanning across the globe—countries with arguably much different values.[151] Following the *Google Spain* ruling, which only

144. Juzgado Nacional de Primera Instancia [1a Inst.] [Court of First Instance], 29/7/2009, "Da Cunha Virginia c. Yahoo de Argentina SRL y otro s/ Daños y perjuicios," No. 75, Expte. No. 99.620/06) (Arg.); *see* Edward L. Carter, *Recent Development: Argentina's Right to be Forgotten*, 27 EMORY INT'L L. REV. 23, 30 (2013).

145. Carter, *supra* note 144, at 25.

146. *Id.* at 25–26.

147. *Id.* at 26.

148. *Id.* at 28.

149. Camara Nacional de Apelaciones en lo Civil de la Capital Federal [CNCiv.] [National Court of Civil Appeals of the Federal Capital], sala D, 10/8/2010, "Da Cunha Virginia c/ Yahoo de Argentina SRL y otro s/ Daños y Perjuicios," (Arg.); Carter, *supra* note 144, at 28–29.

150. Carter, *supra* note 144, at 30.

151. *See* Chelsea E. Carbone, *To Be or Not To Be Forgotten: Balancing the Right To Know With the Right to Privacy in the Digital Age*, 22 VA. SOC. POL'Y & L. 525, 545 (2015).

applied to countries in the EU, Google extended the right to have personal data delisted to Iceland, Liechtenstein, Norway, and Switzerland.[152] Additionally, similar efforts to recognize the right to be forgotten are being made in Hong Kong, Canada, Russia, South Africa, and South Korea.[153] Such movements only exemplify the high value all individuals place on their privacy, and that the EU may just be the catalyst for vast changes in privacy rights relating to the Internet. This progression of countries following the EU in recognizing the right to be forgotten illustrates that the recognition of this right is only beginning to expand.

III. THE RIGHT TO BE FORGOTTEN AND THE PREVENTION OF DATA BREACHES

Data breaches have far-reaching consequences that affect not only the individuals who had their personal data compromised but the companies whose systems were breached as well.[154] The consequences are both social and economical. There is ongoing tension between websites and users of websites with users wanting to have more privacy rights, and social media websites constantly changing their privacy policies.[155] Recognizing a right to be forgotten would allow users to be able to manage their own personal data and lessen their worry over the ever-changing privacy policies of websites and the further sharing of information, which gives hackers more opportunity to breach security systems and retrieve personal information on individuals that the hackers are not authorized to access.

Although it is hard to feel sympathy for the Ashley Madison users who had their data compromised, the point is not a moral one. It is not that these people had affairs, and thus deserved to have their information revealed; the point is that these individuals had their personal security breached and their private information made public without their consent. Ashley Madison charged its users $19 USD to "delete" their information and netted millions

152. *See Legal Help, Search Removal Request Under Data Protection Law in Europe*, GOOGLE, https://support.google.com/legal/contact/lr_eudpa?product=websearch (last visited Feb. 21, 2016); Carbone, *supra* note 151, at 545.

153. *See, e.g.*, Carbone, *supra* note 151, at 545 (Hong Kong's privacy Chief is looking to pressure Google into extended similar privacy safeguards to the region).

154. *See* Jett III & Sloan, *supra* note 13, at 38.

155. Brian Fung, Your Facebook Privacy Settings Are About To Change. Again, WASH. POST, Apr. 8, 2014, https://www.washingtonpost.com/news/the-switch/wp/2014/04/08/your-facebook-privacy-settings-are-about-to-change-again/.

from this fee.[156] The cost to users was more than a dollar amount when the "full delete" did not suffice.[157] Ashley Madison's willingness to charge users to delete personal information demonstrates that the information they kept on users was unnecessary. The cost to ALM has the potential to be astronomical as law firms have filed numerous suits against ALM and Ashley Madison for hundreds of millions of dollars.[158] The costs to Ashley Madison also include the launch of a "full investigation utilizing independent forensic experts and other security professionals to assist with determining the origin, nature, and scope of this attack."[159] Emotionally, the breach has taken a toll on undoubtedly millions of users.[160] The list of emotional and economic impacts is long and has extended further than just to the users of Ashley Madison—the breach has negatively affected the families of these users.[161]

If there were a more global recognition of a right to be forgotten, users would not have had to pay to have their information deleted. The recognition of a right to be forgotten would allow users to decide and take back whatever information they made available to the public. There would be less confusion as to what their rights are if it was laid out in one law since every site has a different privacy policy, and the ability to continually change that policy. With such control, individuals would be able to lessen the amount of information shared online, and give hackers less avenues to gain access to such information.

If information is unnecessary to retain, corporations should give individuals the control to decide whether it stays in the digital world. If a site, such as Ashley Madison, would make users pay to delete information, that information, it would be fair to assume, is unnecessary. If the right to be forgotten existed in more countries, including the United States, information could be taken down more easily from websites. Consequently, when embarrassing personal information is released in an almost inevitable data breach, users may have no one to blame but themselves, hackers aside. Since hackings are becoming more commonplace, it is a risk one takes when allowing your information to be stored electronically.

---

156. Alex Hern, *Ashley Madison Database Suggests Paid-Delete Option Left Identifiable Data Intact*, GUARDIAN, Aug. 19, 2015, http://www.theguardian.com/technology/2015/aug/19/ashley-madisons-paid-delete-option-left-data-identifying-users-post-claims.

157. *Ashley Madison Privacy Breach*, *supra* note 31.

158. Basu, *supra* note 38.

159. Press Release, 18 Aug Statement from Avid Life Media Inc., Ashley Madison media room (Aug. 18, 2015), http://media.ashleymadison.com/statement-from-avid-life-media-inc-august-18-2015/.

160. *See supra* Part I.A.

161. *See id.*

Additionally, the recognition of a right to be forgotten would limit the power of hackers. If the websites where the information was being published were considered data controllers, the information could be removed, assuming the individual's right to privacy outweighs the need to know by society. Furthermore, if links to compromised information could no longer be searched by allowing for the right to be forgotten to apply to search engines, hackers would lose their platform. Taking the Ashley Madison data breach as an example, the main threat from the hackers was releasing the personal information of the websites users, which caused shame for many users and even the extortion of some. The stolen data would have been more difficult to locate for most individuals if links to the information were delisted from search engines, there would have been less shame for individuals, and extortionists would not have had as easy access to the data. The idea of disallowing the publication of illegally obtained information is not a new one, and allowing for the removal of publicized stolen data from websites is a modified branch of the disallowance of publication of illegally obtained materials.

Having users pay to get their information deleted may have netted Ashley Madison a good chunk of money, but its cost is much more than what they gained after the site's data breach. The lawsuits underway will cost society and those involved much time, money, and stress. Ashley Madison essentially charged users for the right to be forgotten, and it backfired.

Whether the law changes, or companies' policies change by allowing users to easily and efficiently delete their information and giving users a right to be forgotten, the effect of data breaches would be less consequential since more of the blame would shift onto the data subject since he or she would have had more control. Ultimately, if users have the right to put up information, they should have the right to take it down.

IV. BRIDGING THE GAP BETWEEN THE UNITED STATES AND THE EUROPEAN UNION

The web provides a place to instantly share information across borders, including personal data. With this unrestrained sharing across borders, it is important to have some congruency between privacy laws in the United States and the EU. The United States and EU have different views on privacy. American privacy law consists of *ad hoc* legislation and regulations and

has no comprehensive privacy legislation,[162] while the EU has a comprehensive framework outlining privacy rights afforded to its citizens—the 1995 Directive.[163] Opponents against the recognition of an individual's right to be forgotten in the United States often cite the First Amendment as their main argument.[164] These opponents argue the right's potential chilling effect on free speech, claiming that such a right will censor what is posted shared on the web.[165] They argue the "right to be forgotten," as enacted in the EU, would be unconstitutional in the United States because it clashes with the First Amendment.[166]

The United States has more protections for freedom of expression than privacy rights: an individual's freedom of expression is expressly protected by the Bill of Rights, though no such protection exists for an individual's privacy rights.[167] However, the right to be forgotten can easily be tailored to align with the strong emphasis Americans place on the freedom of speech and freedom of expression. There are numerous ways to bridge the gap between EU and American ideals of privacy with regards to the right to be forgotten.

A. How the Right to Be Forgotten Could Look in the United States

The EU allows the removal of information for broad purposes, such as being "inaccurate, inadequate, irrelevant or excessive," where the U.S. is far more limiting.[168] However, in the United States, the removal of personal information is, in fact, permitted for some purposes, demonstrating that the erasing of personal information already occurs in some cases.

The First Amendment limits and even prohibits some forms of expression and speech; therefore, the First Amendment should not be an absolute block against the implementation of a right to forgotten in the United States.[169] However, the argument that search-engine results are speech and thus

---

162. Rustad & Kulevska, *supra* note 15, at 376–77.

163. *See generally* Directive 95/46/EC, *supra* note 66.

164. Robert G. Larson III, *Forgetting the First Amendment: How Obscurity-Based Privacy and a Right To Be Forgotten are Incompatible With Free Speech*, 18 COMM. L. & POL'Y 91, 119 (2013).

165. Stuart, *supra* note 59, at 465.

166. Rustad & Kulevska, *supra* note 15, at 416.

167. Emily Adams Shoor, Note, *Narrowing the Right to be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation*, 39 BROOK. J. INT'L L. 487, 498 (2014).

168. Amelia Rufer, *The Creeping "Right to be Forgotten"*, NEWS MEDIA AND THE LAW (Winter 2015), https://www.rcfp.org/browse-media-law-resources/news-media-law/news-media-and-law-winter-2015/creeping-right-be-forgotten.

169. *See What Does Free Speech Mean?*, U.S. COURTS, http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does (last visited Jan. 24, 2016).

protected under the First Amendment from government regulation still stands, which may pose a hurdle in applying the right to be forgotten to include search engines.[170] Although the Supreme Court of the United States has repeatedly stated the First Amendment applies to legally obtained material,[171] the same Court has found that illegally obtained material can be published so long as the publisher was not the one who illegally obtained the material.[172] The obvious problem with such an ideal is that there is an incentive for people to illegally obtain personal data and sell it to someone that can publish it. Furthermore, Section 320 of the Communications Decency Act protects users and providers of interactive computer services who publish information provided by others from liability if that information is harmful, illustrating another reason why the right to be forgotten must be tailored from its EU form to fit within the U.S. legal system.[173] The right to be forgotten in its European form would need to be narrowed in the United States, but both proposed and enacted laws show that the right to be forgotten is not entirely impeded by the First Amendment or Section 230 of the Communications Decency Act in the United States.

California's law on a minor's right to be forgotten illustrate that the right to be forgotten is not necessarily an unwanted right in the United States. The crucial part of the law, however, is that it only applies to content the minor personally gives out, with a few minimal exceptions, as previously discussed.[174] The law allows minors to ask for removal of content they upload to a website, but does not ask for search engines to delist links.[175] This law could be modified to allow for all individuals, not just minors, to be able to permanently remove content they share themselves. Further, the balancing test adopted by the Court in *Google Spain v. AEPD*, which balances an individual's right to privacy and the information's interest to the public, could be used in determining whether or not the information that an individual made public can be removed.[176] People often share or make things public

170. *See* Jian Zhang v. Baidu.com Inc., 10 F. Supp.3d 433, 438 (S.D.N.Y.2014) ("[T]here is a strong argument to be made that the First Amendment fully immunizes search-engine results from most, if not all, kinds of civil liability and government regulation.").

171. *See, e.g.*, Cox Broad. Corp. v. Cohn, 420 U.S. 469, 496–97 (1974).

172. Bartnicki v. Vopper, 532 U.S. 514, 517–18 (2001).

173. 47 U.S.C. § 230 (2016). "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." *Id.* § 230(c)(1).

174. *See* CAL. BUS. & PROF. CODE §§ 22580–81 (2015).

175. *See id.*

176. *See Google Spain*, *supra* note 80, ¶ 31.

that they did not intend to, or share information they now wish to take back, and in an age where such information can remain published indefinitely, there must be some means to take it back. In the case of the Austrian law student who received over 1200 pages of personal information retained by Facebook, it is hard to argue that society has a right to know, or would even want to know, what events he responded to and how he responded. Moreover, that might be information he did not even want recorded in the first place. The extent of information about individuals stored by websites is vast and seemingly unnecessary.

The Consumer Privacy Bill, as previously discussed, also recognizes that privacy rights must adapt with ever-changing technology. The bill focuses on individual control and transparency.[177] Although not enacted, it recognizes that privacy is still valued, and that there needs to be more controls over protecting the privacy of individuals.[178] To follow the guidelines provided in the Consumer Privacy Bill, some have suggest that online marketers collecting users' personal data should have explicit privacy policies outlining how the users' personal data will be used, and that the data held should be held securely as to protect customer information in the event of a data breach.[179] Further, customers should have the ability to prevent companies from using their personal data in certain ways.[180] The Consumer Privacy Bill is consistent with the ideals behind recognizing a right to be forgotten, that is, to allow users to have more control and limit what of their personal data is shared or retained. With a right to be forgotten, the ability to prevent companies from using personal information in certain ways should come with the ability to take back personal data.

Further, the APPS Act also paves the way for a right to be forgotten in the United States. Like the Consumer Privacy Bill, the APPS Act requires transparency in connection with mobile applications and personal data.[181] It also allows for the withdrawal of consent to the collection of personal data.[182] These facets of the APPS Act also show the ideal of privacy still exists in America. The APPS Act further shows how a right to be forgotten could be adapted in the United States, by allowing users to request the mobile application developer to delete stored personal data collected by the application.[183] The right to be forgotten in the United States could

177. *See Consumer Privacy Protection Act* § 101.
178. *See id.* § 3.
179. Andrew Lustigman & Adam Solomon, *An Overview and the Impact of the Consumer Privacy Bill of Rights*, INSIDE COUNSEL (Mar. 12, 2015), http://www.insidecounsel.com/2015/03/12/an-overview-and-the-impact-of-the-consumer-privacy.
180. *Id.*
181. *See generally* H.R. 1913.
182. *Id.* § 2(b).
183. *Id.*

extend the APPS Act to websites and give users the option to request removal of their personal data.

Numerous laws and legislative proposals demonstrate that a right to be forgotten is not impossible in the United States. The right to be forgotten could follow and tailor itself to conform to already existing laws in the United States. The right to be forgotten could encompass allowing users of sites to permanently delete information they provide themselves, allowing users to control how their personal data will be collected, used, and shared, as well as requiring data controllers to allow data subjects to request removal of information collected on them and request the removal of private information uploaded by others that was meant to remain private. With the requests, a balancing test similar to the one adopted by the EU should be adopted, which will be discussed below.

Looking at the Ashley Madison case, if a right to be forgotten existed in the United States in a limited scope, such as allowing users to have information they upload permanently deleted, users would not have had to pay for this removal, that information would not have been kept in relation to payment details and account holders, and less information would have been released. Thus, in future hacks, blame would shift on to users since they had the control over the information that stayed stored.

B. The Balancing Test

The EU has developed a balancing test in *Google v. AEPD*.[184] The test balances the individual's right to privacy against the public's interest in the information being requested for removal.[185] This idea of balancing the right to privacy with public interest has been previously recognized in the United States. In *Landmark Communications, Inc. v. Virginia*, where a newspaper published an accurate article concerning an investigation into a state judge by the Virginia Judicial Inquiry and the Review Commission, the Court refused, on a matter of public concern, to punish the newspaper.[186] One policy concern was that it is in the public's interest to know whether or not elected judges are corrupt.[187] Looking into whether there is a public interest to know the information or if the information is of public concern

184. *See Google Spain*, *supra* note 80, ¶ 31.
185. *See id.* ¶¶ 31, 128.
186. *See* Landmark Communications v. Virginia, 435 U.S. 829, 836 (1978).
187. *See id.*

is included in the test offered in *Google v. AEPD*.[188] Information that is concerning to the public may not be deleted under the right to be forgotten framework in the EU.[189]

The balancing test could be adopted by websites, regulatory committees, and the courts. Currently, the United States does not have a sole regulatory authority that oversees data protection laws.[190] Websites could offer a form, like Google offers for its EU citizens, to request deletion of information. Individuals would have to offer an explanation to why the information is no longer relevant, and the website could weigh it against the interest society would have in the information. If the United States created a regulatory agency for the oversight of data protection and privacy, users could appeal to the agency and the agency could rule whether the information should be removed by applying the same balancing test. Failure of websites to comply with the regulatory agencies ruling could then result in legal processes, leaving it to the courts to apply the balancing test and ultimately decide.

Using Ashley Madison as an example, if a right to be forgotten existed, users of Ashley Madison could have requested that personal information the website stored be deleted. The website, as Google currently does for their EU domains, could balance whether the interest of the individual to have the information remain private is outweighed by society's interest in the information, and if users disagree with a websites decision, they could report it to a regulatory agency.[191] Since much of the information that was to remain private was compromised, such as credit card numbers and names, it would likely have found that the data subjects right to privacy is outweighed by societies interest in having the information kept. Google already offers the allowance of requests to remove certain personal information, such as credit card numbers, even to United States citizens.[192]

Arguably, having such a system would create added administrative costs, as each request would have to be addressed on an individual basis, but it would likely be less costly than the cost of a lawsuit or multiple lawsuits, like the current ones filed against Ashley Madison, as previously outlined.[193]

---

188. *See Google Spain*, *supra* note 80, ¶ 31.
189. *See id.* ¶¶ 31, 128, 106.
190. Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* GETTING THE DEAL THROUGH: DATA PROTECTION AND PRIVACY, 169, 191 (Rosemary P. Jay ed., 2014).
191. *See supra* Part II.A.3.
192. *See Search Help, Removal Policies*, GOOGLE, https://support.google.com/websearch/answer/2744324 (last visited Feb. 15, 2016).
193. Basu, *supra* note 38.

C. Non-Legislative Avenues to Recognize a Right to Be Forgotten

Before any change in legislation, there are multiple non-legislative ways to recognize the right to be forgotten in the United States. Websites on their own could recognize this right before any legislative change takes place and give users the ability to permanently delete information they provide, while users of websites could pressure websites to give more controls to the user. Furthermore, websites could allow users to determine automatic expiration dates for the storage of personal information.

Conforming policies in America to fit into a EU prospective is not a novel idea. American-based websites are already conforming their policies and actions to the privacy laws of the EU since they have EU users, without U.S. legislation requiring such steps. Take, for example, the "Cookie Directive", European Union Directive 2009/136/EC, that requires websites to have consent from their visitors on the sites use of cookies,[194] data that websites store on electronics through browsers to allow for tracking of an individual's actions while using the browser.[195] Websites use cookies for various reasons including user identification, remember previously entered information, and targeted advertising—using information on what a website user has searched for and showing relevant advertisements to such behavior.[196] Some American-based websites have taken the initiative to warn about the websites use of cookies to all users,[197] and some have even given users the means to allow or deny the use of cookies.[198] This demonstrates American companies are compliant with EU privacy laws even though they may be more stringent. Steps can be taken by website operators to recognize a right to be forgotten.

Some companies have already begun to allow for the permanent deletion of personal data users upload themselves. Facebook now allows users to

194. Council Directive 2009/136, 2009 O.J. (L 337) 11 (EC) [hereinafter Cookie Directive].

195. *Cookies*, EUROPA, http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm (last visited Jan. 23, 2016).

196. *Id.*

197. *See Cookies & Other Storage Technologies*, FACEBOOK, https://www.facebook.com/help/cookies/ (last visited Jan. 23, 2016); CNN uses a popup alerting site uses of policy changes and gives a link to their privacy policy, which includes an explanation on their use of cookies. *See CNN Privacy Policy*, CNN, http://www.cnn.com/privacy (last visited Jan. 23, 2016).

198. *See Twitter's Use of Cookies and Similar Technologies*, TWITTER, https://support.twitter.com/articles/20170514 (last visited Jan. 23, 2016).

delete their accounts, rather than just deactivate them.[199] A deactivated Facebook account prevents people from seeing your information on your profile and searching for your profile, but all of your information is still saved by Facebook.[200] A deleted account deletes information posted by the user, such as photos and status updates, but does not include the deletion of information others have shared about the user, nor sent messages.[201] This is the only avenue Facebook allows for the management of personal information stored and used by Facebook,[202] and although it is a step in the right direction, social media websites should allow users to have more control over their information without having to fully delete their entire account.

Users of websites can push for the recognition of a right to be forgotten by essentially recognizing the right themselves. That is, pressuring and demanding websites to allow for more control and the ability to have their information erased. Giving data subjects the ability to delete information they post themselves gives control back to the data subject and would not be as administratively taxing as having websites filter through erasure requests. Had Ashley Madison allowed for user control like this, the effects of the data breach would not have been as large, as people would not have had to pay for an unsuccessful service and their information could have been removed when they felt it was no longer relevant or needed. Individuals who had fake accounts made using their personal information would have had easier avenues to try and get that information permanently erased if they became aware of the account existing under their name or e-mail. With more controls, the blame would have been shifted to the users since they were the ones with the power over what information was stored since we live in a world where data breaches are a reality.

Another proposed idea is to have expiration dates on how long personal information will remain stored.[203] Under this idea, the data subject would be able to choose how long information they post will be stored before it is automatically deleted, and third parties would no longer have access to the information after the designated time.[204] This idea gives users more control over their personal information and allows for the discontinuation of perpetual storage. Had this system been implanted by Ashley Madison, less data would have been shared with the public, and again, more blame

199. *Facebook Data Policy*, *supra* note 3.
200. *Id.*
201. *Id.*
202. *Id.*
203. Rustad & Kulevska, *supra* note 15, at 382.
204. *Id.*

would be shifted onto the users since they would have had a controlling part in what information was stored.

V. CONCLUSION

In a world where what you do is immortalized on the web, there needs to be increased safeguards surrounding it. People often change their ideals, behavior, and opinions, but when it is left on the web, it is not forgotten. Information that was thought to be private now has to potential to come back and reach a larger scale of people, which can have a sizable negative effect on a data subject—effects from humiliation to suicide. Certain individuals have learned how to extort private information that has come into their hands, such as those extortionists that used information from the Ashley Madison hack to blackmail users, by making data subjects pay to get their private information taken down.

The right to be forgotten is accepted in the EU, and since the *Google v. AEPD* ruling, the right to be forgotten has expanded in the EU, allowing for individuals to request information third parties uploaded to be delisted from Google. This arguably may go too far to be adopted in the United States, but the United States does not entirely disregard the idea of a right to be forgotten. The United States has witnessed recent developments towards the recognition of a right to be forgotten by giving minors the right to have their personal information that they post deleted, by creating revenge porn laws, by drafting the Consumer Privacy Bill, and by the introduction of the APPS Act. These recent developments show that a more limited form of a right to be forgotten in the United States is not unfathomable. The right to be forgotten in the United States could allow for users to permanently delete personal information they provided themselves and control how their personal information is collected and used. In addition, websites could take requests for the removal of personal data collected on data subjects along with requests to remove private personal data on an individual published by another user. These websites could then use a balancing test to weigh an individual's privacy right against society's interest in having access to the information when deciding whether or not to accept or deny the request.

In an age where data breaches are inevitable, adopting a right to be forgotten can lessen the effects of such breaches. With such a right, data subjects would have more control over their own personal data, and consequently, at the time of a data breach, blame would be shifted to the data subject his or herself for the information they allowed the breached

website to store. Accordingly, the European idea of a right to be forgotten can certainly be applied in the United States, but in a more limited scope.