THE RIGHT TO BE FORGOTTEN:

AN ANALYSIS FROM AN AMERICAN PERSPECTIVE AND WHAT IT MEANS FOR THE U.S. TO ADOPT IT

Ani Kristo

14 December 2018

ABSTRACT

Today's society is part of a shared digital life, with an Internet population of 3.2 billion people. Though this colossal data infrastructure enables communication, information sharing, and collaboration, it is a place that favors a paradigm of continuous collection and storage of data, without much analysis of how that disrupts certain social norms and induces cases of violations of fundamental rights like privacy, freedom, and protection from discrimination.

In 2016, the European Union adopted the General Data Protection Regulation, which introduced a right for individuals to have their personal data erased. This opened a discussion on privacy and identity concerns in the context of perpetual stigmatization and discrimination due to obsolete data that remains on the web. Through analyses of some cases in the U.S. and E.U., this paper will investigate the challenges of importing a similar legal framework for the erasure of personal data in the U.S., while ensuring the freedom of expression and maintaining the quality of the search engines and respective websites.

TABLE OF CONTENTS

1. INTRODUCTION

The Information Age has led to an exponential increase in data collection from both private companies and government agencies. Thanks to the ubiquitous inter-connectivity brought by the Internet, user data is now easily captured, collected, and stored in massive data centers for its preciousness in automatic knowledge discovery and applications of pattern recognition in the marketing realm. Consequently, the storage centers keep growing as data is always stored by default, and not forgotten. Looking at the last few years, this has caused personal data to be too vulnerable to security breaches like the notorious incidents at Yahoo,[1] Equifax,[2] eBay,[3] Adobe,[4] and Cambridge Analytica.[5]

Despite being conscious that modern technology enables for unprecedented forms of data matching, de-anonymization, and mining, users are often unaware of what sorts of operations their data goes through, nor do they have control over how it is used. In addition, most service providers use vague and inaccessible terms in their software agreements, which results in another opaque wall for the average user of their products, consequently contributing to the creation of extensive digital dossiers.[6] While many observers in the U.S. used to perceive digital redemption as entirely unworkable and ridiculous, after the Snowden revelations, the general public has begun to consider the idea more seriously.[7]

---

1. Nicole Perlroth, "Yahoo Says Hackers Stole Data on 500 Million Users in 2014," September 2016, https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

2. Seena Gressin, "The Equifax Data Breach: What to Do," September 2017, https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

3. Gordon Kelly, "eBay Suffers Massive Security Breach, All Users Must Change Their Passwords," May 2014, https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/.

4. Brad Arkin, "Important Customer Security Announcement," October 2013, https://theblog.adobe.com/important-customer-security-announcement/.

5. Emma Graham-Harrison and Carole Cadwalladr, "Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach," March 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

6. Meg Leta Ambrose and Jef Ausloos, "The right to be forgotten across the pond," *Journal of Information Policy* 3 (2013): 1–23.

7. "Forgetting Made Impossible," in *Ctrl + Z: The Right to Be Forgotten*, by Meg Leta Jones (NYU Press, 2016), 55–80, ISBN: 9781479881703, http://www.jstor.org/stable/j.ctt1803zhx.6.

Incentivized by these and additional issues, in 2016, the European Union adopted the General Data Protection Regulations (G.D.P.R.)[8] - a massively complex law aimed at regulating data protection and privacy for E.U. citizens, as well as personal data export by service providers outside the European Economic Area. In Article 17, this new law introduces the *Right to Erasure*, more commonly referred to as the *Right to Be Forgotten*, as a basic and universal right for all data subjects[9]. It asserts that data subjects have the right to request the removal of their personal data from any data controller without undue delay.[10] The law specifies cases when this right is applicable, including when the personal data is no longer necessary for the purposes for which it was collected and when the data subject revokes their consent. If the personal data has been publicized, the regulations require the data controller[11] to "take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure [...] of any links to, or copy or replication of, those personal data".[12]

One of the main use-cases for the safeguards that G.D.P.R. provides is that of protection against *perpetual stigmatization* as a consequence of a specific action performed in the past. Individuals whose personally identifiable information is still present and discoverable by online services in the context of unflattering events, such as arrests or public scandals, could be subject to ostracism and discrimination from employers or creditors. In these cases, the Right to Be Forgotten allows them to request the online erasure of their past,

8. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," *Official Journal of the European Union* L119 (May 2016): 1–88, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

9. Article 4 of the G.D.P.R. defines the term 'data subjects' as an "identified or identifiable natural person", - in other terms - a user of an online service whose data is present (given or collected) in the service provider's storage facilities.

10. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 17.

11. Article 4 of the G.D.P.R. defines the term 'data controller' as "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".

12. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 17.

after a reasonable amount of time has passed, and at a point when the information would no longer bear interest for the public. In addition, this right extends facility for protection against instances of cyberbullying, non-consensual pornography, and the commercial use of arrest information, by enforcing online service providers to build this functionality as an inherent part of their products.

To date, the United States has not adopted this right and there are no legal frameworks that directly grant data subjects that degree of control over their personal data online. Although there have been public and legal debates on this subject matter, the First Amendment rights, specifically freedom of speech, have always trumped any claim to privacy when data was truthful, used fairly, and collected in a legal manner. However, American companies that operate in the E.U. and provide online services for E.U. citizens are required to abide to the G.D.P.R. and have started adopting measures that respect such regulations. Therefore, the question whether the U.S. will adopt the Right to Be Forgotten has not necessarily reached closure.

In this paper I will provide an analysis of the possibility and feasibility of importing the Right to Be Forgotten in the U.S., through the lens of relevant legal cases in the E.U. and U.S. and look at possible solutions that reconcile these conflicting views.

2. BACKGROUND ON G.D.P.R.

European lawmakers and courts have a long history of protecting privacy. In 1995, at the time when Internet was still at infancy, the European Council issued the Data Protection Directive[13] "on the protection of individuals with regard to the processing of personal data and on the free movement of such data", which was superseded, in 2016, by a more comprehensive reform called the General Data Protection Regulation (G.D.P.R.), which enlists provisions that are better suited for the modern technologies and the recent data usage

13. Council of European Union, *Directive 95/46/EC*, 1995, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

trends in the online world. Today, the G.D.P.R. is regarded as a gold standard for privacy protection laws around the world in these times of a technological revolution.[14]

The G.D.P.R. defines the term 'personal data' as "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[15] However, Viviane Reding, Vice-President of the European Commission and EU Commissioner for Justice, proposed a slightly modified definition for the type of data that the G.D.P.R. should protect. She stated that if we limit the notion of data to the "information that the consumers have voluntarily given out to the online service providers", then it is easier to require controllers to manage the references in media or anywhere else, while respecting the state-specific laws for the freedom of expression.[16] This definition of data falls under the first category, according to the data type classification of chief privacy counsel of Google, Peter Fleischer, who thinks that this makes space for a "legally enforceable right that is mostly symbolic and entirely unobjectionable".[17]

Among a long of list of requirements and provisions, the G.D.P.R. introduces the *Right to Data Portability*, the *Right to Not Be Profiled* and the *Right to Be Forgotten*, which empower online users with the ability to have full control over giving and withdrawing consent on how their personal data is used and requesting erasure of its online presence. The *Right to Data Portability* maintains that data subjects have the right to receive all the personal data concerning them in a structured and portable format that can easily be

14. "The History of the General Data Protection Regulation," https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

15. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 4.

16. John Hendel, "Why Journalists Shouldn't Fear Europe's 'Right to be Forgotten'," January 2012, https://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/.

17. Peter Fleischer, "Foggy thinking about the Right to Oblivion," March 2011, http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

transmitted to other data controllers.[18] On the other hand, data subjects have the *Right to Not Be Profiled*, which means that, unless explicit consent is given, the users shall not be subject to any form of automated processing of personal data to analyze or predict aspects concerning their performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.[19] Thirdly, the most interesting and controversial[20] provision of the G.D.P.R. is the *Right to Erasure (Right to Be Forgotten)*, which is:

> ... the right to obtain from the controller the erasure of personal data concerning him or her without undue delay ....[21]

This right is a more thorough version of *Le droit à l'oubli*, a French law from 2010, presented in *Chartes du droit à l'oubli numérique*[22] - an initiative from Nathalie Kosciusko-Morizet, aiming at defining the rights of citizens with respect to targeted advertising enabled by the data collection of individuals without their full knowledge, and the regulation of the personal results displayed by search engines.

This right, however, only pertains to the protection of *personal data*, as defined above, and is applicable on a *best effort* standard for data controllers[23]. In addition, the G.D.P.R. gives data controllers the ability to refuse the user's request for the erasure of personal data by enumerating a set of exemptions, including the cases when the data is necessary to exercise the right of freedom of expression and information, for reasons of public interest

18. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 20.

19. Ibid., Article 22.

20. Paul Voigt, "The compliance burden under the GDPR," September 2016, https://globaldatahub.taylorwessing.com/article/the-compliance-burden-under-the-gdpr-data-protection-officers; *The Committee's opinion on the European Union Data Protection framework proposals*, vol. 1 (2012), 33–34, https://publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/572.pdf.

21. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 17.

22. ""Droit à l'oubli" sur Internet : une charte signée sans Google ni Facebook," October 2010, Original archive link: http://www.prospective-numerique.gouv.fr/sites/default/files/CP_SignatureCharteDAOsitescollaboratifsetmoteursderecherche_13_10_2010.pdf, https://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html.

23. Article 17 of the G.D.P.R. simply states that data controllers "shall take reasonable steps" to remove personal data, hence indicating a lack of guarantee that the subject's request will be partially or fully granted.

in the area of public health, scientific or historical research or statistical purposes, and for the establishment, exercise or defence of legal claims.[24]

Beginning 25 May 2018, the G.D.P.R. is enforceable - directly binding and applicable - upon all the online service providers that which are based in the E.U. or whose users are citizens of the E.U.. This means that data collecting and processing companies in the U.S., such as Google or Facebook, will also need to comply to this regulation if they operate in the E.U., hence, forthbrining an elaborate discussion on whether the U.S. should adopt this right while maintaining its constitutionality in the context of freedom of speech.

3. THE CENTRAL DEBATE IN THE U.S.

The Right to Be Forgotten is only applicable in cases when personal data is previously made publicly available, hence differing from the more general *Right to Privacy*, as alluded by Warren and Brandeis,[25] and exercisable for private data under the logical extension of the Fourth Amendment to digital properties. However, the Right to Be Forgotten does contradict the right to express one's opinions without restraint, as outlined in the First Amendment of the Bill of Rights. Therefore, in the U.S., any request made under this right could be interpreted as an attempt to censorship, hence violating the freedom of expression. Hitherto attempts by judges, legislators, and advocates to etch out some space for privacy concerns in the light of the reverence for expression, explicitly granted in the Constitution, have been woefully unsuccessful.[26]

Moreover, there is an inherent dimension of time in any claims to exercise the Right to Be Forgotten. The G.D.P.R. recognizes that the passage of time is one of the main factors in judging the necessity for the continuation of data processing by the controller.[27] However,

24. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 17.

25. Samuel D Warren and Louis D Brandeis, "The right to privacy," *Harvard law review*, 1890, 193–220.

26. "Forgetting Made Impossible."

27. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)," Article 17, p 1(a).

the U.S. law that concerns these cases has no notion of 'expiration' of the freedom of speech after that content has been consumed, so, arguably, there must exist a way of establishing a balance between the individual and public interests from a temporal perspective.

Given that the introduction of this right primarily affects the press, journalistic organizations have also participated in this discussion, with the New York Times warning that such a powerful right could impede journalists and dissidents from getting their voice heard and this "purge" will eventually leave the public less well informed.[28]

Furthermore, The Economist takes the discussion beyond the aspect of civil liberties when they identify the enormous burden of compliance for small companies, which, in this current state of technology where A.I.-enhanced software is primarily data-driven, "would keep technology companies from innovating".[29] Though, the very idea that the current technological trends of innovation are profoundly dependent on the collection of personal data could be the core problem that the G.D.P.R. is addressing.

On the other hand, the arguments from the parties advocating the Right to Be Forgotten mainly consist in that permanent storage of all sorts of personal information may be subject to a large-scale data cross-referencing that could fuel up abusive, biased, and discriminatory software classification systems, subsequently contributing to the establishment of an Orwellian structure. Supporters of the Right to Be Forgotten even include prestigious journals in Europe, which have applauded the European Commission's decision to arbitrate an effective system that allows the exercising of this right. *El País* writes: "In a democratic society, where even criminal records can be canceled after a while, the Internet could become a life sentence for some people".[30] The German daily *Der Spiegel* describes the ruling as

28. "Ordering Google to Forget," *The New York Times*, May 2014, https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?_r=0.

29. "America should borrow from Europe's data-privacy law," April 2018, https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

30. "Derecho al olvido," *El País*, May 2014, https://elpais.com/elpais/2014/05/13/opinion/1400007067_055407.html.

"a victory over the omnipotence of American Internet companies and a victory of the value placed by the people of the Old World against the economization of the private sphere".[31]

Nonetheless, the general opinion in the U.S. remains strongly negative towards the import of the Right to Be Forgotten. Andrew McLaughlin, former head of global public policy for Google and deputy chief technology officer for the Obama Administration, has called this "an epically bad decision, a travesty, an example of great moral and institutional failure on the part of the European Union itself". He asserts that the suppression of true information, that is not libel or meant as hate speech, will only favor the interests of well-connected elites in Europe, who have a particularly strong concern in hiding embarrassing facts about their lives.[32]

On a similar note, Jonathan Zittrain, professor of International Law and Computer Science at Harvard University, insists that the Right to Be Forgotten is a bad solution to a real problem since "the incentives are clearly lopsided towards content removal" without oversight or penalty provisions for improper removals, which will easily lead companies to fulfill takedown requests without much selectivity, consequently decreasing the quality of content on the Internet.[33]

3.1. Existing legal frameworks in the U.S.

While the U.S. law does not directly grant citizens the Right to Be Forgotten, there exists a four-prong framework for handling content removal requests on a case-by-case basis. Under the Intellectual Property restrictions and Copyright laws, users can prevent the replication of content created by the information subject, but they only reach the creative aspects of that work and do not reach information created by another person related to the data sub-

31. "Europe: 1, Google: 0: EU Court Ruling a Victory for Privacy," *Der Spiegel*, May 2014, http://www.spiegel.de/international/business/court-imposes-right-to-be-forgotten-on-google-search-results-a-970419.html.

32. February 2015, https://www.intelligencesquaredus.org/debates/us-should-adopt-right-be-forgotten-online.

33. Ibid.

ject.[34] In addition, Section 107 of the DMCA[35] permits the use of copyrighted material in situations that are considered fair use, including criticism, comment, news reporting, teaching, scholarship, or research, hence rendering the IP and copyright mechanisms unsuitable for cases when the personal data that is exposed on the web does not have an artistic nature or is used fairly.

Secondly, another legal mechanism that can be utilized to control the flow of personal information online is that of contractual obligations, such as Non-Disclosure Agreements. However, the restrictions only apply to persons privy of the contract, whereas much of the online information about the data subjects occur outside of that relationship.

Thirdly, subjects wishing to have their personal data removed can follow the avenue of defamation claims when the information damages their reputation. Unfortunately, information genuineness is an absolute defense in these cases and, in many instances, courts have maintained that public interest and newsworthiness are not necessarily diminished with the passage of time.[36]

Finally, the privacy torts (intrusion upon seclusion, public disclosure of private facts, misappropriation, and false light[37]), despite being relevant to digital redemption, are usually successful in obstructing the distribution or access to information only if it is in the interest of the public, and not on an individual level, where the damages occur from continued access to personal information.[38]

Even though there is no U.S. law that can provide the same benefits as the G.D.P.R.'s Right to Be Forgotten, there exist multiple privacy-protecting regulations that work in different contexts, such as the Fair Credit Reporting Act of 1970,[39] the California Consumer

34. *Copyright law of the United States of America: contained in Title 17 of the United States Code* (Library of Congress, U.S. Copyright Office), http://uscode.house.gov/browse/prelim@title17.
35. Ibid., Section 107.
36. *Sidis v. FR Pub. Corporation*, 1940, 806; *Estill v. Hearst Publishing Co.*, 1951, 1017; *Perry v. Columbia Broadcasting System, Inc.*, 1974, 797; *Street v. National Broadcasting Co.*, 1981, 1227.
37. William L Prosser, *Law of torts* (1971).
38. "Forgetting Made Impossible."
39. *Fair Credit Reporting Act no 91-508* (The 91st United States Congress, 1970).

Privacy Act of 2018,[40] the Privacy Act of 1974 for medical records,[41] Title XI for the U.S. Code (U.S. Bankruptcy Code),[42] pardons, and statutes of limitation, which protect the privacy of consumers, the use of credit information, and limit the effect of stigma by preventing the use of such information for employment discrimination.

The lack of a U.S. legal framework that is equivalent to the G.D.P.R. in the context of the Right to Be Forgotten does not suggest, however, that U.S. legislators have not considered or attempted to import this right. Specifically, the New York Assembly Bill 5323[43] and Senate bill 4561[44] were introduced in February 2017 by Assemblyman David I. Weprin and State Sen. Tony Avella with the purpose of rectifying an individual's reputation that was wrongly diminished through inaccurate information found on the Internet by mandating that:

> Upon the request from an individual, all search engines, indexers, publishers and any other persons or entities that make available, on or through the internet information about the requester, shall remove information, articles, identifying information and other content about such individual that is "inaccurate", "irrelevant", "inadequate", or "excessive" within thirty days of such request.[45]

These bills were, however, not enacted on the grounds that the proposals were too broad, rely on a vague test based on what the government *thinks* the public should or should not be discussing, and is clearly unconstitutional under current First Amendment law since it protects the power to suppress speech.[46]

The Obama Administration also prepared a blueprint for a Consumer Privacy Bill of Rights in their 2012 as part of a comprehensive report to improve consumers' privacy

40. *California Consumer Privacy Act no 1798.100*, AB-375 (2017-2018 Session) (2018).

41. *Privacy Act no 93-579*, 88 Stat. 1896 (The 93rd United States Congress, 1974).

42. *Bankruptcy Code of the United States of America: contained in Title 11 of the United States Code*, http://uscode.house.gov/browse/prelim@title11.

43. *An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act no A05323* (The New York State Assembly, 2017).

44. *An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act no S04561* (The New York State Senate, 2017).

45. Ibid.

46. Eugene Volokh, "N.Y. bill would require people to remove 'inaccurate,' 'irrelevant,' 'inadequate' or 'excessive' statements about others," March 2017, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others.

protections and ensure that the Internet remains an engine for innovation and economic growth.[47] The outlined framework introduces protections over what personal data organizations collect from data subjects and how they use it by requiring collectors to provide transparency, respect for the context, secure data handling, focused collection, and accountability.[48] This proposal has not moved forward since it would not give the F.T.C. the authority to enforce the principles, instead, make companies and industry associations write their own rules and then ask the F.T.C. to sign off on them, potentially overturning state laws that offer stronger protections.[49]

4. Relevant cases

Historically, there have been multiple lawsuits in the U.S. whose central claim has been the removal of content that has caused reputation damage. The examples vary in the type of the personal data that was used as well as the platform bearing such data. The following are some highlights of lawsuits that had the same nature as the content protected by the Right to Be Forgotten in the G.D.P.R.

Melvin v. Reid In 1931, the appellate court in Melvin v. Reid, held that the use of the real name of a prostitute in the movie "The Red Kimono", depicting her murder trial in 1918, was "unnecessary" and harmful, since it had caused her ridicule and exposed her to obloquy, hence upholding the plaintiff's claim that it violated her right to privacy. The court's main argument relied on the fact that "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".[50]

Sidis v. F-R Publishing In this case, the court denied the claims of Sidis, a former child prodigy, that an article of great public interest, published by the defendant, had in-

47. The White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (February 2012).

48. Ibid., p.10.

49. Brendan Sasso, "Obama's Privacy Bill of Rights Gets Bashed from All Sides," February 2015, https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

50. *Melvin v. Reid*, 1931, 91.

truded upon his privacy by recounting his breakdown and the revulsion which the plaintiff thereafter felt for his former life of fame and study.[51]

Liberty Lobby, Inc. v. Pearson In this case from 1967, the judge denied the plaintiff's request for an injunction for the publication of the contents of some letters that contained private and confidential information about the plaintiffs, which is one of the central scenarios that the G.D.P.R.'s Right to Be Forgotten now protects users against.[52]

Briscoe v. Readers Digest Association Later on, in 1971, the California Supreme Court in the case of Briscoe v. Readers Digest Association, decided that the exposure of a criminal who paid their debt to the society and started a new, law-abiding life, without sufficient reason connected to the current events of public interest, constituted an invasion of their privacy.[53]

Throughout the years, the attitudes in case-specific decisions have changed sometimes in favor of the Right to Erasure and mostly not. In fact, Melvin v. Reid and Briscoe v. Readers Digest Association are two of the very few cases when these sorts of claims have won over the freedom of expression. Therefore, it is not quite right to argue that there has been a gradual tendency towards one end of the rope in this tug of war. However, it was not until the landmark case of Google Spain v. AEPD in 2014 when the discussion around truthful content removal from published sources was thought of through the lens of a Right to Erasure, which would be later be popularized as the Right to Be Forgotten.

4.1. Google Spain v. AEPD and Mario Costeja González

The history of the Right to Be Forgotten in the E.U. starts with a decision of the European Court of Justice for the case of Google Spain v. the Spanish Data Protection Agency (A.E.P.D.) and Mario Costeja González. On the order of the Spanish Ministry of Labour and Social Affairs, a Spanish newspaper called *La Vanguardia* published two announcements regarding the forced sale of Costeja's properties arising from his social security

51. *Sidis v. FR Pub. Corporation.*
52. *Liberty Lobby, Inc. v. Pearson*, 1967, 489.
53. *Briscoe v. Reader's Digest Association, Inc.*, 1971, 34.

debts. Arguing that the sale had been closed a long time ago and that it carried no further relevance, Costeja asked Google Spain to remove links to the announcement of the newspaper appearing from a Google search of his name.[54]

Eventually, the court ruled that an individual may request links to be removed from the search engine's index search and that engines are processors of personal data and, as such, are responsible for taking the necessary steps to hide the digital footprint of the data in concern. In addition, the court ruled that the information in question must be obsolete, seriously harmful, and belonging to a person with no public relevance or historical significance.[55]

In this monumental case, we see the first attempt at defining the scope of accountability for the the data controllers, which was extended to search engines, and not the direct publishers, because the impact on personal privacy of journalistic media articles is lower than the impact caused by the revelation of universal results afforded by a search engine, which makes it possible to build up a complete profile of the affected individual.[56]

If this case were to be carried out in the U.S., Costeja's claims would most probably be unsuccessful because of First Amendment's interpreted priority and Google's immunity from liability as a search platform as described in Section 230 of the Communications Decency Act, which treats search engines simply as conduits and prevents them from being "treated as the publisher or speaker of any information provided by another information content provider".[57]

5. Open challenges and solutions

Many challenges still exist in the aspects of understanding the scope and enforcing accountability in the process of exercising of the Right to Be Forgotten. The primary questions is

54. *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González*, 2014, 131/12.

55. Ibid.

56. Marina Santín, "The problem of the right to be forgotten from the perspective of self-regulation in journalism," *El profesional de la información (EPI)* 26, no. 2 (2017): 303–310.

57. *Communications Decency Act of the United States of America: contained in Title 47 of the United States Code*, Section 230, http://uscode.house.gov/browse/prelim@title47.

whether the online service providers should proactively take the necessary measures to track the flow of personal data, record the intermediate conduits in the process, and take the necessary measures to be able to execute an erasure request swiftly and fully; or, alternatively, take a more reactive approach by evaluating and operating on a case-by-case basis. While the former is ideal for the end-users, it would introduce an enormous implementation barrier for businesses since it demands a big infrastructural upgrade that incurs massive costs. In addition, this would result in a bigger collection of meta-data, which partly contradicts the essence of exercising the Right to Be Forgotten.

Secondly, it is unclear to what extent data channel operators should be held accountable for the erasure procedures. The G.D.P.R. does not explicitly enlist what type of the provided services would qualify the controllers as responsible for taking the necessary steps to fulfill an erasure request. The definition of the protected personal data in Article 17 implies that the direct publisher will be responsible for the erasure, however, it is ambiguous whether that extends to the providers of third-party references to the publishing authority (i.e. the sharing of a link or the the whole content of personal data within the service platform, outside the platform through the utilities of the publisher, or outside of the platform through other utilities provided by external applications or operating systems).

In addition, there is no predefined erasure strategy that clarifies whether the critical content should be permanently removed, stored in a dormant server and hidden from public access, or just hidden from "naïve" users' access but still reachable through specific, detailed, and explicit search queries or similar operations.

Moreover, with an increasing number of modern hardware and software tools that extend the capabilities of the traditional data-mining algorithms, a new set of methods of re-identification and de-anonymization are being invented.[58] Therefore, it appears that the sole redaction of the personal identifiable information, as defined in Article 4 of the

58. Melissa Gymrek et al., "Identifying Personal Genomes by Surname Inference," *Science* 339, no. 6117 (2013): 321–324, ISSN: 0036-8075, doi:10.1126/science.1229566, eprint: http://science.sciencemag.org/content/339/6117/321.full.pdf, http://science.sciencemag.org/content/339/6117/321; Arvind Narayanan and Vitaly Shmatikov, "Robust de-anonymization of large sparse datasets," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on* (IEEE, 2008), 111–125; Arvind Narayanan and Vitaly Shmatikov, "How to break anonymity of the netflix prize dataset," *arXiv preprint cs/0610105*, 2006,

G.D.P.R. and cited in Section 2 of this paper, is not enough to hide the identity of individuals, nor does it prevent future providers from programmatically making inferences about their identity by utilizing these re-identification algorithms that work on publicly available information or auxiliary data. Consequently, this burdens the Data Protection Officers with unreasonable liability and responsibility for being aware of all the contemporary methods of maliciously restoring the hidden identity of the protected data subjects, and continuously taking measures to provide up-to-date protection of the personal data in a climate of fast-paced technological advances and scientific research on Big Data. Unfortunately, this onerous duty for the controllers might render the current legal framework for data erasure to be simply a half measure for what should be a complete and effective, but currently unfeasible, personal data protection framework.

If the U.S. were to adopt the Right to Be Forgotten in some manner, then it will have the opportunity to establish more transparent guidelines and feasible restrictions by improving over the G.D.P.R. in the aforementioned topics. Despite the fact that most of the big corporations that deal with massive social networks and perform innovative large-scale personal data processing are based in the Silicon Valley, the U.S. has yet to actively contribute to the discussion of possible solutions for the issues above. Nevertheless, there is potential for using this right as a template in the U.S. by building upon its shared constitutional values.

6. PROPOSED SOLUTIONS

In her speech about data protection in the digital age, Commissioner Reding admitted that "it is clear that the Right to Be Forgotten cannot amount to a right of the total erasure of history",[59] and, especially in the U.S., that sentiment is strongly intertwined with the absolute nature of the freedom of expression.

The only way of reconciling these two opposing forces is to rely upon a collection of measures - computer code, technical design, market forces, government regulations,

59. Viviane Reding, *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, January 2012, http://europa.eu/rapid/press-release_SPEECH-12-26_en.pdf.

norms, and other social regulators - to jointly govern these values, since none of them can be deemed a silver bullet.

One of the non-legal alternatives is employing tools like reputation management services (e.g. Reputation.com[60], Reputation Defender®[61], and Integrity Defenders[62]) which are a form of PR or brand management for individuals. This alternative to the Right to Be Forgotten maintains the right of the content creators (e.g. journalists) to freely express their thoughts, while providing reputation repair by oversaturating the online presence of a data subject with content from a large number of trust-affirming transactions. These services do not necessarily present more accurate, relevant, or valuable information, but they offer a way to counterpoise damaging content. However, the truth remains that this "strong-arming" method is not effective for subjects wishing to have real seclusion, nor does it offer a feeling of empowerment with privacy.

Probably the most effective solution to having a system of managing the online presence of a data subject is to provide preventative tools that incorporate *forgetfulness-by-design*. This implies that the service software be engineered to automatically destroy data according to some time-decay model that works like memory in human brains, or by using timers that dictate for how long the data will be accessible from the system. For example, Snapchat, a popular messaging app, is entirely built around the promise of "... empowering people to express themselves [and] live in the moment...",[63] which is enabled by allowing users to set self-destruction timers for their images and videos. Moreover, Telegram, another popular messaging app, has a feature of 'secret chat', which accomplishes the same functionality of data ephemerality for text messaging. On the other hand, online services whose data model is not compatible with a concept of lifetime or expiration, may use a decaying function that simulates the human forgetfulness with the passage of time, and then use this to bury older data deeper into the search result listings or by simply increasing the difficulty of the discovery of that data.

60. https://www.reputation.com/
61. https://www.reputationdefender.com/
62. http://integritydefenders.com/
63. "Snap Inc.," http://www.snap.com/.

It is evident that a big redesign that accommodates these trade-offs needs a longer discussion and understanding from all the involved stakeholders, however, there is space for immediate action for the initiation of a process of increasing awareness and caution on the side of the users. Seth P. Berman from Harvard Law calls for more accessible software use terms and bigger transparency for the end-user operations that the personal data is processed for. In addition, he advocates the idea that the U.S. government should create a liability scheme for data privacy, clarifying the accountability of data controllers.[64] On the other hand, content creators, including news reporters at Reporters Without Borders, encourage media's self-regulation and the strict adherence to journalistic ethics that can act as a preventative measure of concealing personal data that is not necessary for the purpose of reporting.[65]

Above all, multiple scholars like danah boyd, Jeffrey Rosen, and Julian Togelius, experts in socio-technical research, observe that society will adjust to this revolution of technology that has brought new paradigms of data processing. They claim that people will come up with coping mechanisms as a solution to digital forgetting, such as the creation of new norms of atonement, forgiveness through empathy, and increasing the acceptability of closeted skeletons by becoming capable of ignoring them or judging less harshly.[66]

7. Conclusion

In this paper I gave a brief overview of a new provision of the General Data Protection Regulation, namely the Right to Be Forgotten, which aims to give online users the ability to manage their online presence in an era of continuous and massive data collection. This new protection was generally applauded in the European Union and is considered a triumph of civil liberties against the 'evil', data-hungry American companies. Even though the

64. Seth P. Berman, "GDPR in the U.S.: Be Careful What You Wish For," May 2018, http://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html.

65. Santín, "The problem of the right to be forgotten from the perspective of self-regulation in journalism."

66. Frank D Fincham, Julie H Hall, and Steven RH Beach, "Til lack of forgiveness doth us part: Forgiveness in marriage," *Handbook of forgiveness*, 2005, 207–226; Caryl E Rusbult et al., "Forgiveness and relational repair," *Handbook of forgiveness*, 2005, 185–205.

United States has historically embraced a culture of 'going west' - loosening the shackles of the past and seeking a new place of redemption and re-invention of oneself - the Right to Be Forgotten remains controversial in the U.S., with a low probability that the legislators devise a similar legal framework due its argued unconstitutionality with respect to the First Amendment rights. Quoting on the court ruling of Time Inc. v. Hill, a good summary of the American attitude towards this right is that "The risk of exposure is an essential incident of life in a society which places a primary value on freedom of speech and of press".[67]

However, even though the U.S. does not have a similar regulation for data controllers, American companies whose primary business model relies on personal data processing are required to comply to the G.D.P.R. as long as they serve to E.U. citizens or operate in the E.U. This has led to a general increase of awareness of the legal and ethical issues from both the customers and providers side, in addition to encouraging a bigger discussion of data hygiene, organization, mindfulness, accountability, and risks. Though, the critics believe that this is not enough, and that "if America continues on today's path, it will fail to protect the privacy of its citizens and long-term health of its firms".[68]

Even though the G.D.P.R. is a very comprehensive set of regulations for data protection in the E.U., when it comes to the Right to Be Forgotten, there are still a lot of open challenges that come with the rapid development of technological tools, for which there is no obvious legal solution that is general enough to work agnostically with any kind of online service providers and keep up with adversarial methods that could potentially antagonize digital redemption and forgetfulness. However, there exist non-legal solutions that accommodate both sides of the central debate in the U.S. and ensure a sustainable future for online users' seeking data erasure, as well as for service providers wishing to maintain their business objectives by keeping their customers happy and appreciated.

67. *Time, Inc. v. Hill*, 1967, 374.
68. "America should borrow from Europe's data-privacy law."

REFERENCES

Ambrose, Meg Leta, and Jef Ausloos. "The right to be forgotten across the pond." *Journal of Information Policy* 3 (2013): 1–23.

An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act no A05323. The New York State Assembly, 2017.

An act to amend the civil rights law and the civil practice law and rules, in relation to creating the right to be forgotten act no S04561. The New York State Senate, 2017.

Arkin, Brad. "Important Customer Security Announcement." October 2013. https://theblog.adobe.com/important-customer-security-announcement/.

Bankruptcy Code of the United States of America: contained in Title 11 of the United States Code. http://uscode.house.gov/browse/prelim@title11.

Berman, Seth P. "GDPR in the U.S.: Be Careful What You Wish For." May 2018. http://www.govtech.com/analysis/GDPR-in-the-US-Be-Careful-What-You-Wish-For.html.

Briscoe v. Reader's Digest Association, Inc., 1971.

California Consumer Privacy Act no 1798.100. AB-375 (2017-2018 Session). 2018.

Communications Decency Act of the United States of America: contained in Title 47 of the United States Code. http://uscode.house.gov/browse/prelim@title47.

Copyright law of the United States of America: contained in Title 17 of the United States Code. Library of Congress, U.S. Copyright Office. http://uscode.house.gov/browse/prelim@title17.

Council of European Union. *Directive 95/46/EC*, 1995. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

"Europe: 1, Google: 0: EU Court Ruling a Victory for Privacy." *Der Spiegel*, May 2014. http://www.spiegel.de/international/business/court-imposes-right-to-be-forgotten-on-google-search-results-a-970419.html.

"Derecho al olvido." *El País*, May 2014. https://elpais.com/elpais/2014/05/13/opinion/1400007067_055407.html.

Estill v. Hearst Publishing Co., 1951.

"The History of the General Data Protection Regulation." https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

"Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)." *Official Journal of the European Union* L119 (May 2016): 1–88. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC.

Fair Credit Reporting Act no 91-508. The 91st United States Congress, 1970.

Fincham, Frank D, Julie H Hall, and Steven RH Beach. "Til lack of forgiveness doth us part: Forgiveness in marriage." *Handbook of forgiveness*, 2005, 207–226.

Fleischer, Peter. "Foggy thinking about the Right to Oblivion." March 2011. http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html.

"Forgetting Made Impossible." In *Ctrl + Z: The Right to Be Forgotten*, by Meg Leta Jones, 55–80. NYU Press, 2016. ISBN: 9781479881703. http://www.jstor.org/stable/j.ctt1803zhx.6.

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014.

Graham-Harrison, Emma, and Carole Cadwalladr. “Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach.” March 2018. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

Gressin, Seena. “The Equifax Data Breach: What to Do.” September 2017. https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do.

Gymrek, Melissa, Amy L. McGuire, David Golan, Eran Halperin, and Yaniv Erlich. “Identifying Personal Genomes by Surname Inference.” *Science* 339, no. 6117 (2013): 321–324. ISSN: 0036-8075. doi:10.1126/science.1229566. eprint: http://science.sciencemag.org/content/339/6117/321.full.pdf. http://science.sciencemag.org/content/339/6117/321.

Hendel, John. “Why Journalists Shouldn’t Fear Europe’s ’Right to be Forgotten’.” January 2012. https://www.theatlantic.com/technology/archive/2012/01/why-journalists-shouldnt-fear-europes-right-to-be-forgotten/251955/.

House, The White. *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*. February 2012.

Kelly, Gordon. “eBay Suffers Massive Security Breach, All Users Must Change Their Passwords.” May 2014. https://www.forbes.com/sites/gordonkelly/2014/05/21/ebay-suffers-massive-security-breach-all-users-must-their-change-passwords/.

“”Droit à l’oubli” sur Internet : une charte signée sans Google ni Facebook.” October 2010. https://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html.

Liberty Lobby, Inc. v. Pearson, 1967.

Melvin v. Reid, 1931.

Narayanan, Arvind, and Vitaly Shmatikov. "How to break anonymity of the netflix prize dataset." *arXiv preprint cs/0610105*, 2006.

———. "Robust de-anonymization of large sparse datasets." In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, 111–125. IEEE, 2008.

Perlroth, Nicole. "Yahoo Says Hackers Stole Data on 500 Million Users in 2014." September 2016. https://www.nytimes.com/2016/09/23/technology/yahoo-hackers.html.

Perry v. Columbia Broadcasting System, Inc., 1974.

Privacy Act no 93-579. 88 Stat. 1896. The 93rd United States Congress, 1974.

Prosser, William L. *Law of torts*. 1971.

Reding, Viviane. *The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, January 2012. http://europa.eu/rapid/press-release_SPEECH-12-26_en.pdf.

Rusbult, Caryl E, Peggy A Hannon, Shevaun L Stocker, and Eli J Finkel. "Forgiveness and relational repair." *Handbook of forgiveness*, 2005, 185–205.

Santín, Marina. "The problem of the right to be forgotten from the perspective of self-regulation in journalism." *El profesional de la información (EPI)* 26, no. 2 (2017): 303–310.

Sasso, Brendan. "Obama's Privacy Bill of Rights Gets Bashed from All Sides." February 2015. https://www.theatlantic.com/politics/archive/2015/02/obamas-privacy-bill-of-rights-gets-bashed-from-all-sides/456576/.

Sidis v. FR Pub. Corporation, 1940.

"Snap Inc." http://www.snap.com/.

Street v. National Broadcasting Co., 1981.

The Committee's opinion on the European Union Data Protection framework proposals. 1:33–34. 2012. https://publications.parliament.uk/pa/cm201213/cmselect/cmjust/572/572.pdf.

"America should borrow from Europe's data-privacy law." April 2018. https://www.economist.com/leaders/2018/04/05/america-should-borrow-from-europes-data-privacy-law.

"Ordering Google to Forget." *The New York Times*, May 2014. https://www.nytimes.com/2014/05/14/opinion/ordering-google-to-forget.html?_r=0.

, February 2015. https://www.intelligencesquaredus.org/debates/us-should-adopt-right-be-forgotten-online.

Time, Inc. v. Hill, 1967.

Voigt, Paul. "The compliance burden under the GDPR." September 2016. https://globaldatahub.taylorwessing.com/article/the-compliance-burden-under-the-gdpr-data-protection-officers.

Volokh, Eugene. "N.Y. bill would require people to remove 'inaccurate,' 'irrelevant,' 'inadequate' or 'excessive' statements about others." March 2017. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/15/n-y-bill-would-require-people-to-remove-inaccurate-irrelevant-inadequate-or-excessive-statements-about-others.

Warren, Samuel D, and Louis D Brandeis. "The right to privacy." *Harvard law review*, 1890, 193–220.