122 PENN STATE LAW REVIEW PENN STATIM 1

Is the European Right to Be Forgotten Viable in the Land of the First Amendment?

Andrea Gallinucci-Martinez*

TABLE OF CONTENTS

***

* J.D., University of Bologna, 2014; LL.M., King's College London, 2014; LL.M., Columbia Law School, 2017. I wish to dedicate this work to my wife Tanya, my mother Cinzia, and my father Carlo. I wish to thank Jonathan Donnellan, who helped me understand the American individualism in relation to freedom of expression and of the media. Every single one of our conversations enriched my perspective on the relationship between First Amendment, press and society, often changing my original stance on various issues. I am extremely grateful for such an amazing and challenging experience, and hope this work reflects my efforts.

122 PENN STATE LAW REVIEW PENN STATIM 1

ABSTRACT

In this article, I argue that the preferred way to shape an American right to be forgotten is to grant users the control of their online personal data via expressed contractual obligations included in the terms of use and conditions of internet service providers. To pave the road to that assessment, I first discuss the evolution of the right to be forgotten in Europe, the competing values behind its creation, and the current scope and limits of the right. Then, I analyze whether a 2017 bill introduced in the New York State Assembly that expressly mirrors the European right to be forgotten can survive First Amendment constitutional muster. After having concluded that the bill would not pass the constitutional test, I examine whether and to what extent considering the right to be forgotten as an implied contractual obligation between users and service providers represents a viable theory for shaping an American version of the European right to be forgotten. Finally, in light of the recent Cambridge Analytica scandal and the entry into force of the General Data Protection Regulation, I argue that it is time to rethink online privacy in terms of expressed contractual obligations.

Introduction

Whether we fully realize it or not, we live in a society governed by algorithms.[1] The law and its interpretation, however, still appear anchored to traditional values and principles that do not properly account for the drastic changes posed by the internet and its tools.[2] This certainly is the case when it comes to privacy and freedom of speech in the online arena, where the judicial exercise of balancing competing rights produces interesting and unique outcomes that differ from one normative framework to

[1] *See* Brian Simpson & Maria Murphy, *Editorial, Technological challenges and opportunities: the future of law*, 25(1) INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 1, 1 (2016) ("In a time where algorithms are making decisions that affect every citizen … it is important to address how such changes will affect society and to consider what role, if any, law should play in the regulation and use of new technologies and internet services.").

[2] *See* Pamela Samuelson, *Five Challenges for Regulating the Global Information Society*, in *Regulating the Global Information Society* 317, 317 (Chris Marsden ed. Routledge, 2000), available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=234743 ("When old laws do not fit and cannot easily be adapted, it may be necessary to go back to first principles and consider how to accomplish societal objectives in the new context of the Internet.").

another.[3] This work focuses on the right to be forgotten ("RTBF"), offering a comparative analysis of its alternate fortune in Europe and in the United States of America.

In section A of this article, I discuss the evolution of the RTBF in Europe, the competing values behind its creation, and the current scope and limits of the right. In section B, I analyze whether a recent bill (the "Bill")[4] introduced in the New York State Assembly in 2017 that expressly allows individuals to request removal of online information about themselves "that is inaccurate, irrelevant, inadequate or excessive" directly quoting the language used by the Court of Justice of the European Union in *Google Spain* at § 92,[5] can survive First Amendment constitutional muster. In section C, I examine whether and to what extent considering the RTBF as an implied contractual obligation between users and service providers represents a viable theory for shaping an American version of the European RTBF. In section D, in light of the recent Cambridge Analytica scandal and the entry into force of the General Data Protection Regulation,[6] I argue for the introduction of expressed contractual obligations in internet service providers' terms of use and conditions as a preferred way to create a viable and effective American RTBF.

---

[3] *See* Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECHNOLOGY REVIEW (April 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology/ ("We haven't come to grips with what is ethical, let alone with what the laws should be, in relation to technologies such as social media. Consider the question of privacy. Our laws date back to the late 19th century when newspapers first started publishing personal information … [and] gaps in privacy laws have grown exponentially since then.").

[4] *See* bill no. S04561, available at: http://nyassembly.gov/leg/?default_fld=&leg_video=&bn=S04561&term=2017&Summary=Y&Text=Y. See also, the similar bill no. A05323, available at: https://nyassembly.gov/leg/?default_fld=&leg_video=&bn=A05323&term=&Summary=Y&Text=Y.

[5] Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, case C-131/12 (C.J.E.U. May 13, 2014), available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131.

[6] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (available at: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679), which entered into force on May 25, 2018.

The scope of the foregoing analysis will be limited to information that (i) was truthful and accurate at the time of first publication, and (ii) involve private figures.

A. Evolution, Scope and Limits of the RTBF in Europe: Balancing Competing Values

The RTBF is understood as "the right of an individual to erase, limit, or alter past records that can be misleading, redundant, anachronistic, embarrassing, or contain irrelevant data associated with the person, likely by name, so that those past records do not continue to impede present perceptions of that individual."[7] This description is the product of a remarkably nuanced and recent evolution in the field of online data protection and privacy that dramatically changed the landscape of individual rights and journalism in the internet era. However, the scope and strength of the RTBF were (and still are, in many ways) surrounded by uncertainty when confronted with competing values, like freedom of expression and information.[8]

In 2009, *Times Newspapers v. the United Kingdom*[9] revealed the European Union's initial approach to the RTBF.[10] This case did not directly concern the RTBF; the main issue resolved by the court involved the affirmation of the so called "internet publication rule" (*i.e.*, each publication amounts

[7] Michael J. Kelly & David Satola, *The Right to Be Forgotten*, 2017 U. ILL. L. REV. 1, 3 (2017).
[8] *See* Noam Tirosh*, Reconsidering the 'Right to be Forgotten' – memory rights and the right to memory in the new media era*, 39(5) MEDIA, CULTURE & SOCIETY 644, 651 (2017) (stating the RTBF "created a harsh debate between advocates of privacy rights and those of expression rights.").
[9] Times Newspapers Limited (Nos. 1 and 2) v. the United Kingdom, E.Ct. H.R., 10 March 2009, appl. no. 3002/03 and no. 23676/03, available at http://www.openmediacoalition.it/documenti/echr-case-of-times-newspapers-ltd-nos-1-and-2-v-the-united-kingdom/index.html.
[10] *See* Cécile de Terwangne, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, REVISTA DE INTERNET, DERECHO Y POLITICA 109, 113 (2012) ("In … the Times Newspapers case, the European Court of Human Rights shed some very interesting light on how the [RTBF] balancing test should be implemented.").

to a separate cause of action) over the "single publication rule", which provides the plaintiff with a single cause of action for all the defamatory content published in any jurisdiction.

Nonetheless, in dicta, the European Court of Human Rights recognized that "while the primary function of the press in a democracy is to act as a 'public watchdog', it has a valuable secondary role in maintaining and making available to the public archives containing news which has previously been reported."[11] In fact, internet archives can substantially contribute to preserving and making available news and information for education and historical purposes, and the press has a "duty … to act in accordance with the principles of responsible journalism by ensuring the accuracy of … information published" in its online archives. [12]

The foregoing view seemed to value accuracy of information instead of privacy; rather than forcing online search engines to make online information inaccessible (or hard to locate), interested individuals could ask the author to revise its content, providing follow-up information that more accurately reflected the current status of affairs. Such a framework would ensure accuracy of information not only at the time of first publication, but throughout its availability in online archives. For example, a former convicted individual whose information pops up on an online search engine many years after the occurrence of certain criminal events could ask the owner of the online database to revise her story in light of her befallen redemption. Drawing from this model, news would not be considered as a set-in-stone and immutable historical event, but rather as a constantly evolving narrative, which

[11] *Times Newspapers*, at 45.
[12] *Id.*

integrates the past with the present without necessarily having a lifespan.[13] Over time, however, accuracy of information was outweighed by privacy concerns, creating a privacy-oriented RTFB.[14]

In 2012, EU's Justice Commissioner Viviane Reding noted that even tiny scraps of personal information could affect people long after being divulged; thus, individuals should be able to protect their privacy by deciding whether or not to provide certain personal data to the public.[15] However, she continued, the RTBF should not be treated as "an absolute right. There are cases where there is a legitimate and legally justified interest to keep data in a database. The archives of a newspaper are a good example. It is clear that the right to be forgotten cannot amount to a right of the total erasure of history. Neither must the right to be forgotten take precedence over freedom of expression or freedom of the media."[16]

This privacy-centered view was later championed by the 2014 Court of Justice of the European Union (hereinafter also referred as "CJEU")'s *Google Spain* decision.[17] The CJEU, in fact, shaped the current boundaries of the RTBF in the EU by creating an individual right that overrides, as a rule, both

[13] In relation to the concept of lifespan of information, *see generally*, Viktor Mayer-Schönberger, Chapter VI: Reintroducing Forgetting, in *Delete: The Virtue of Forgetting in the Digital Age 104* (Princeton University Press, 2011).
[14] *See* Tirosh, *supra* note 8, at 650 (stating the European RTBF "was developed as a privacy issue.").
[15] *See The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age*, Press release of EU's Justice Commissioner Viviane Reding on January 22, 2012, available at: http://europa.eu/rapid/press-release_SPEECH-12-26_en.htm ("[p]eople need to be able to make an informed decision about what to disclose, when and to whom.").
[16] *Id.*
[17] For a comprehensive analysis of *Google Spain*, *see* John W. Kropf, *Note, Google Spain SL v. Agencia Española de Protección de Datos (AEPD). Case C-131/12*, 108(3) THE AMERICAN JOURNAL OF INTERNATIONAL LAW 502 (2014). *See also* Global Freedom of Expression – Columbia University, *Note, Google Spain SL v. Agencia Española de Protección de Datos*, https://globalfreedomofexpression.columbia.edu/cases/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos-aepd/.

the interests of the operator of the search engine and of the public in the availability of online content relating to someone's name.[18]

The case originated from a complaint made by Mr. Costeja González, a Spanish private citizen who, in 1998, was mentioned in two articles published by a Spanish newspaper in relation to a real-estate auction connected with attachment proceedings for the recovery of social security debts against him. In 2009, after realizing that when searching his name on Google.com the resulting index linked to the two articles, Mr. González reached out to the newspaper to ask for the removal of such material, arguing that the proceedings were concluded years earlier without any outstanding issue. After the newspaper refused to take down the disputed content, in 2010 Mr. González contacted Google Spain to request deletion of any links to the articles that resulted from a search of his name on Google's search engine.

When Google declined to comply with his request, Mr. González filed a formal complaint with the Spanish Data Protection Agency (hereinafter, "AEPD"), requesting two remedies. First, that the newspaper be compelled "to remove or alter those pages so that the personal data relating to him no longer appeared or to use certain tools made available by search engines in order to protect the data. Second, … that Google Spain or Google Inc. be required to remove or conceal the personal data relating to him so that they ceased to be included in the search results and no longer appeared in the links" associated with the newspaper.[19] The AEPD dismissed the claims against the newspaper because

[18] *See Google Spain* at 97.
[19] *Id.* at 15.

publishing information concerning the auction proceedings was lawful and justified by the goal of achieving "maximum publicity [for] the auction in order to secure as many bidders as possible."[20] However, the AEPD upheld the claims against Google because "operators of search engines are subject to data protection legislation" and, as a result, can be required to withdraw or prohibited from accessing data that is capable of "compromis[ing] the fundamental right to data protection and the dignity of persons in the broad sense, [which] encompass[es] the mere wish of the person concerned that such data not be known to third parties."[21]

When Google challenged the AEPD's decision, the Spanish high court (Audiencia Nacional) decided to stay the proceedings and defer the interpretation of the applicable European directive to the Court of Justice of the European Union. The CJEU determined that "the operator of a search engine is obliged to remove from the list of results displayed following a search made on the basis of a person's name links to web pages, published by third parties and containing information relating to that person, also in a case where that name or information is not erased beforehand or simultaneously from those web pages, and even, as the case may be, when its publication in itself on those pages is lawful."[22] However, the CJEU noted that in particular instances an interference with "[t]his fundamental right is justified by the preponderant interest of the general public in having … access to the information in question."[23]

[20] *Id.* at 16.
[21] *Id.* at 17.
[22] *Id.* at 88.
[23] *Id.* at 97.

The above analysis illustrates that the right to privacy and the RTBF are not absolute; they must be weighed against competing rights, such as freedom of information and of the press, to find the appropriate balance between private and public interests.[24] The equilibrium reached in the EU between these competing values had the practical effect of creating a right to "informational autonomy or self-determination … [which] derive[s] from the right to privacy, but not in the classical meaning of 'privacy' read as 'intimacy' or 'secrecy'. It rather refers to another dimension of privacy, that is, individual autonomy, the capacity to make choices, to take informed decisions; in other words to keep control over certain aspects of one's life."[25] By necessity, those individual choices to conceal certain information from the public eye carry an element of coercion: when the RTBF is validly invoked, "its net result is that the person exercising it diminishes, if not censors, the right to information of others … affect[ing] the right to free expression."[26]

Clearly, *Google Spain* values privacy as a right with equal, if not greater, standing than freedom of expression.[27] The interest in protecting personal information from exposure to public scrutiny

[24] *See* Kropf, *supra* note 17, at 505 (noting the Court of Justice of the European Union "effectively ruled that a fair balance must be found between the legitimate interests of Internet users who may be interested in having access to information and the privacy rights of the individuals whose personal data is in question."). *See also* Michael Douglas, *Questioning the Right to Be Forgotten*, 40 ALTERNATIVE L.J. 109, 111 (2015) ("However good the balance struck in Google Spain sounds, reality is something different. By making human rights protection vulnerable to the vicissitudes of the profit motives of multi-national corporations, the process is considerably weakened."). *See also* Michee Smith, *Updating our "right to be forgotten"*, TRANSPARENCY REPORT (February 26, 2018) https://blog.google/topics/google-europe/updating-our-right-be-forgotten-transparency-report/ (noting that since the Google Spain decision in 2014, Google has received 2.4 million requests to delist information and complied with 43.3% of those requests).

[25] Cécile de Terwangne, *The Right to be Forgotten and Informational Autonomy in the Digital Environment*, in *The Ethics of Memory in a Digital Age: Interrogating the Right to be Forgotten* 82, 86 (Alessia Ghezzi et al. (eds.) Palgrave Macmillan, 2014).

[26] *See* Antoon De Baets, *A historian's view on the right to be forgotten*, 30(1-2) INTERNATIONAL REVIEW OF LAW, COMPUTERS & TECHNOLOGY 57, 58 (2016).

[27] *See Google Spain* at 91 ("The data subject may oppose the indexing by a search engine of personal data relating to h[er] where their dissemination through the search engine is prejudicial to h[er] and h[er] fundamental rights to the protection of

outweighs concerns about taking potentially newsworthy content away from the marketplace of ideas. This view reflects the EU's vocation to protect people's individual rights against broader interests, to enhance self-determination, and to guarantee dignity and reputation to the ones who need it the most.[28] The European RTBF affords protection to many individuals who desperately need a second chance from society and crave some sort of redemption. In general, these are people who have historically been disenfranchised and do not have the resources to afford legal expenses or pay private service providers or websites to take down blameworthy online information concerning their past.[29] Without recognition of the RTBF, wealthy individuals or corporations would still be able to privately buy their online privacy, but many average persons would be left with no means to protect their reputation, internalizing all the costs of freedom of expression without enjoying the benefits of having their voices heard by the public.

In summary, the European RTBF is grounded in the protection of privacy as a fundamental yet not absolute right. In fact, the individuals' right to informational self-determination has to be reconciled with the right of the general public to know and have access to content of particular significance. In the

---

those data and to privacy — which encompass the 'right to be forgotten' — override the legitimate interests of the operator of the search engine and the general interest in freedom of information.").

[28] *See* Douglas, *supra* note 24, at 122 ("The values of self-determination and autonomy which underpin the right to be forgotten are only valuable because we are actually free to make choices. We have free will. Thus when embarrassing things happen, we can choose to ignore them, and when accidents happen, we can choose to forgive … Choice is going to become more and more important … We can't forget, but we need forgiveness: it is human nature.").

[29] *See* Joseph W. Jerome, *Response, Buying and Selling Privacy: Big Data's Different Burdens and Benefits*, 66 STAN. L. REV. ONLINE 47, available at https://www.stanfordlawreview.org/online/privacy-and-big-data-buying-and-selling-privacy/ (reporting that in relation to the big data phenomenon, Jerome noticed that "[h]istorically, the poor have had little expectation of privacy—castles and high walls were for the elite, after all. Even today, however, the poor are the first to be stripped of fundamental privacy protections … [and their] self-determination and personal autonomy [is threatened] more than any other class. Even assuming they can be informed about the value of their privacy, the poor are not in a position to pay for their privacy.").

next section, I consider whether this balance could be transposed into the American framework by investigating if the Bill introducing a European-like RTBF could survive constitutional muster in light of the First Amendment's doctrine.

B. The American Framework: Can a Bill Introducing a RTBF Similar to the European RTBF Survive Constitutional Muster?

Google Spain's outcome generated a vibrant debate in the United States,[30] which ultimately led to the introduction of the Bill, in 2017. The Bill directly quoted the language used by the Court of Justice of the European Union in *Google Spain* at § 92, expressly allowing individuals to request removal of online information about them "that is inaccurate, irrelevant, inadequate or excessive." Many have argued that such an attempt to introduce the RTBF via legislation would create a form of censorship most likely to be unconstitutional.[31] Those views are primarily based on the idea that

[30] For a vehement criticism of the Google Spain decision and the European RTBF, *see* Jeff Jarvis, *The right to remember, damnit* (May 30, 2014), https://buzzmachine.com/2014/05/30/right-remember-damnit/ (commenting on the Google Spain decision, Jarvis said "[t]his is a most troubling event for speech, the web, and Europe. The court has trampled the free-speech rights not only of Google but of the sites — and speakers — to which it links. The court has undertaken to control knowledge — to erase what is already known — which in concept is offensive to an open and modern society and in history is a device used by tyrannies; one would have hoped that European jurists of all people would have recognized the danger of that precedent."). For a welcoming approach to the creation of the European RTBF, *see* Richard J. Peltz-Steele, *The 'right to be forgotten' online is really a right to be forgiven,* WASH. POST (November 21, 2014), https://www.washingtonpost.com/opinions/the-right-to-be-forgotten-online-is-really-a-right-to-be-forgiven/2014/11/21/2801845c-669a-11e4-9fdc-d43b053ecb4d_story.html?utm_term=.6f6a93fc2773 (asserting the RTBF "is really a right to be forgiven; a right to be redeemed; or a right to change, to reinvent and to define the self anew. A person convicted of a crime deserves a chance at rehabilitation: to get a job or a loan. A person wrongly charged or convicted deserves even more freedom from search-engine shackles.").

[31] *See, e.g.*, Jonathan Zittrain, *Don't Force Google to 'Forget',* N.Y. TIMES (May 14, 2014), https://www.nytimes.com/2014/05/15/opinion/dont-force-google-to-forget.html?_r=0 (arguing the European RTBF "is a form of censorship … that would most likely be unconstitutional if attempted in the United States."). *See also*, Meg L. Ambrose, *Speaking of Forgetting: Analysis of Possible Non-EU Responses to the Right to be Forgotten and Speech Exception*, 38 TELECOMMUNICATIONS POLICY 800, 805 (2014) (arguing the European RTBF has "uncertain likelihoods of developing in the U.S. without being declared a violation of the First Amendment.").

recognition of an implicit right to privacy has historically fallen flat when faced with the Supreme Court's allegiance to the First Amendment, as proven by a consolidated line of caselaw.[32]

In *Florida Star*,[33] the Supreme Court addressed "[t]he tension between the right which the First Amendment accords to a free press … and the protections that various statutes and common-law doctrines afford to personal privacy against the publication of truthful information."[34] Notably, the Court based its analysis on a trilogy of cases that presented the conflict between truthful reporting and privacy interests: *Cox Broadcasting*,[35] *Oklahoma Publishing*,[36] and *Smith v. Daily Mail*.[37] As a result, the Court formulated a twofold limited holding, expressly clarifying both the negative and positive effects of its opinion. First, the Court explained that it did "not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the individual from intrusion by the press, or even that a State may never punish publication."[38] Then, it positively stated that "where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order."[39]

---

[32] *See* John Hendel, *In Europe, a Right to Be Forgotten Trumps the Memory of the Internet*, THE ATLANTIC (February 3, 2011), http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgottentrumps-the-memory-of-the-internet/70643/ ("In America, the implicit right to privacy always fell flat when running against the Supreme Court's fidelity to the First Amendment.").
[33] Florida Star v. B.J.F., 491 U.S. 524 (1989).
[34] *Id.* at 530.
[35] Cox Broadcasting Corp. v. Cohn, 420 U.S. 469 (1975).
[36] Oklahoma Pub. Co. v. District Court, 430 U.S. 308 (1977).
[37] Smith v. Daily Mail Pub. Co., 443 U.S. 97 (1979).
[38] *Florida Star*, 491 U.S. at 541.
[39] *Id.*

In its reasoning, the Court found that protecting privacy and safety of sexual assault victims did not amount to a highest order interest.[40] However, besides that narrow factual determination, the Court did not offer any criteria on how to apply the *Florida Star* test to different fact-patterns and future invasion of privacy actions.[41] This lack of clarity paved the road for a balancing test strongly tilted toward First Amendment protection of truthful publication, which persisted even when the threats posed to privacy by emerging multimedia platforms and online technology became clear.

Interestingly, Justice White's dissent contended that the majority "hit the bottom of a slippery slope … [b]y holding that only 'a state interest of the highest order' permits the State to penalize the publication of truthful information, and … that protecting [one's] right to privacy [in relation to sensitive information] is not among those state interests of the highest order."[42] Justice White recognized that (i) the right to privacy is not absolute; it inevitably conflicts with the public's right to be informed,[43] and (ii) attempting to strike an appropriate balance between such conflicting interests is a very difficult matter.[44] However, he appeared resolute in stating that the public's right to know must be subject to

[40] *Id.* at 525 ("Although the interests in protecting the privacy and safety of sexual assault victims and in encouraging them to report offenses without fear of exposure are highly significant, imposing liability on the Star in this case is too precipitous a means of advancing those interests.").
[41] *See* Mary E. Hockwalt, *Bad News: Privacy Ruling To Increase Press Litigation, The Florida Star v. B.J.F.*, 23(3) AKRON L. REV. 561, 566 (1990) ("The Florida Star Court's narrow holding fails to provide lower courts with any guidelines to decide future invasion of privacy cases.").
[42] *Florida Star*, 491 U.S. at 550.
[43] *See id.* at 551 ("Of course, the right to privacy is not absolute … [it] inevitably conflicts with the public's right to know about matters of general concern-and that sometimes, the latter must trump the former.").
[44] *See id.* ("Resolving this conflict is a difficult matter, and I fault the Court not for attempting to strike an appropriate balance between the two, but rather, fault it for according too little weight to [the victim's] side of equation, and too much on the other.").

reasonable limitations as far as it concerns individuals' private facts.[45] This conclusion was in line with *Dep't of Justice v. Reporters Committee for Freedom of the Press*,[46] which the Court decided approximately a month before *Florida Star*. In fact, in *Reporters Committee*, the Supreme Court admitted its awareness of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data archives,[47] and recognized the existence of a "privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public."[48]

The concerns expressed by Justice White's dissenting opinion in *Florida Star* were also shared by lower courts. In *Briscoe*,[49] the Supreme Court of California ("SCC") created a distinction between reports of "hot news", which deserve heightened First Amendment protection, and reports of past crimes, whose facts are newsworthy but identification of the actor usually serves little independent public purpose.[50] As the SCC observed, in relation to past events "the great general interest in an unfettered press may be outweighed at times by the interest in affording an opportunity for all but the most infamous [former criminals] to begin a new life."[51] Surprisingly, *Briscoe* pioneered recognition and protection of self-determination, dignity, reputation, and redemption, values that later became essential

[45] *Id.* at 552-553 (White, J, dissenting) ("I would strike the balance rather differently … find[ing] a place to draw the line higher on the hillside: a spot high enough to protect [the survivor's] desire for privacy and peace-of-mind in the wake of a horrible personal tragedy. There is no public interest in publishing the names, addresses, and phone numbers of persons who are the victims of crime-and no public interest in immunizing the press from liability in the rare cases where a State's efforts to protect a victim's privacy have failed.").
[46] DOJ v. Reporters Comm. for Free Press, 489 U.S. 749 (1989).
[47] *See id.* at 770 ("In today's society, the computer can accumulate and store information that would otherwise have surely been forgotten long before a person attains the age of 80.").
[48] *Id.* at 767.
[49] Briscoe v. Reader's Digest Association, Inc., 4 Cal.3d 529 (1971).
[50] *See* Gates v. Discovery Communications, Inc., 34 Cal.4th 679, 686 (2004).
[51] *Id.* at 686.

in *Google Spain*. Unfortunately, the balancing test set forth in *Briscoe* came to represent a minority view, repeatedly undermined by the Supreme Court's First Amendment jurisprudence, and eventually overruled in *Gates v. Discovery Communications Inc.*[52]

The above-mentioned analysis highlights the Bill's weaknesses and illustrates various issues likely to undermine its viability under the U.S. Constitution. First, the First Amendment strongly shields the media's right to publish truthful information lawfully acquired.[53] Second, the Supreme Court's First Amendment jurisprudence—unlike the leading European caselaw—reflects a strong presumption that freedom of information trumps privacy.[54] Third, the only way for states to introduce a "RTBF statute" capable of limiting First Amendment rights would be to create a narrowly tailored means for achieving a compelling state interest of the highest order. The means devised by the Bill is far from being narrowly tailored; according to Volokh, its provisions are broad and vague.[55] Finally, the majority opinion in *Florida Star* suggests that protecting individuals' right to privacy (even in relation to highly sensitive

[52] *See id.* at 685 ("Defendants argue that *Briscoe* has been overruled by subsequent high court decisions, at least with respect to information a publisher obtains from public (i.e., not sealed) official records of judicial proceedings … we agree with defendants.").
[53] *See* Robert K. Walker, *The Right to Be Forgotten*, 64(1) HASTINGS L. J. 257, 276 (2012) ("While truthful publications are not automatically afforded First Amendment protection, there have been no cases where the Court has found an individual's privacy rights are themselves a 'state interest of highest order'.").
[54] *See* Edward Lee, *The Right to Be Forgotten v. Free Speech*, 12(1) I/S: A JOURNAL OF LAW AND POLICY 85, 99 (2015) (observing the Supreme Court "favor[ed] free speech over privacy in most, if not all, cases in which the two interests have been implicated."). *See also*, Walker, *supra* note 53, at 277 ("Given the breath of First Amendment protections following *Florida Star*, the speech rights of creators and third-party websites trump the privacy rights of data subjects.").
[55] *See* Eugene Volokh, *N.Y. bill would require people to remove 'inaccurate,' 'irrelevant,' 'inadequate' or 'excessive' statements about others*, WASH. POST (March 15, 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/?utm_term=.fa19decc0906 ("[T]he deeper problem with the bill is simply that it aims to censor what people say, under a broad, vague test based on what the government thinks the public should or shouldn't be discussing. It is clearly unconstitutional under current First Amendment law, and I hope First Amendment law will stay that way.").

information) would not be considered a state interest of the highest order. For those reasons, the Bill would almost certainly fail to survive constitutional muster.

In the next section, I reflect on whether the current First Amendment's dogma could move towards a more balanced approach, and the extent to which contractual obligations can create some leeway for shaping a constitutionally sound version of the RTBF.

C. RTBF as an Implied Contractual Obligation: Right to Data Deletion

As seen in section B, over time American courts consistently recognized the primacy of the First Amendment over privacy interests. This recurring and unfettered interpretation of the US constitution had the practical effect of transforming the First Amendment into a national anthem, a reason to celebrate, cherish, and be proud of the American individualism in relation to freedom of expression and of the media when compared to other less radical approaches.

In the United States, as a general rule, content that becomes public can rarely return to private. The passing of time can diminish the newsworthiness of certain events, but it cannot impair the presence of a piece of information within the realm of the open marketplace of ideas, to which the public retains access. While in Europe the decision-making power over the dissemination of personal data rests on the individuals affected by the news, in the American framework the fate of online personal information is ultimately left to the editorial judgment of the press.

This contrast is reflected in the idea that in the United States the media industry is charged with the task of "uncover[ing] … and report[ing] … the truth about people" and everyone is entitled to

"discover and discuss the secrets of our neighbors." [56] For these reasons, leaving the authority to decide whether certain information is "inaccurate, irrelevant, inadequate or excessive"[57] to individuals represents a revolution that the U.S. Constitution would not allow, since the balance between First Amendment and privacy has consistently leaned towards imposition of the former over the latter. The basic idea that private persons could decide whether or not some public information about them is worth discussing runs against First Amendment's core values and is irreconcilable with the American legal system. Therefore, if Europe protects its citizens via the introduction of a right to safeguard their privacy, in the United States individuals are charged with the duty of "protect[ing] their own privacy."[58]

Despite the foreseeable defeat of the Bill and the almost unbeatable standing of the First Amendment within the legal arena, a recent survey found that Americans manifested support for a European-style take-down system.[59] As Bode and Jones observed, "[p]eople's preferences … conflict somewhat with established American law, particularly the First Amendment. Whether these preferences will move political players to disrupt established principles and institutions will be a matter of politics and Constitutional interpretation."[60]

---

[56] David Anderson, *The Failure of American Privacy Law*, in *Protecting Privacy* 139, 140 (Basil S. Markesinis ed. Oxford University Press, 1999).
[57] *Google Spain* at 92.
[58] Walker, *supra* note 53, at 271.
[59] *See* Leticia Bode & Meg L. Jones, *Ready to forget: American attitudes toward the right to be forgotten*, 33(2) THE INFORMATION SOCIETY, 76, 81 (2017) (revealing the results of the study show a "greater support for a European-style take-down system that relies on search engines to make determinations, rather than putting a government agency in charge."). *See also* Chris J. Hoofnagle et al., *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?*, 20, EDUCATION N.Y. (April 14, 2010), available at http://educationnewyork.com/files/547597-00005-54505.pdf ("[Y]oung-adult Americans have an aspiration for increased privacy even while they participate in an online reality that is optimized to increase their revelation of personal data.").
[60] Bode & Jones, *supra* note 59, at 82.

Personally, I do not see this pivotal change happening with the current roster of Justices, nor do I envision it in the near future. However, fifty years from now societal needs may be different; well-established legal doctrines and interpretations could tremble under the pressure posed by technology, and competing values and interests could be balanced in new and unexpected ways. After all, as the Supreme Court of Canada stated in *Pro Swing Inc. v. Elta Golf Inc.*, "[t]he law and the justice system are servants of society, not the reverse."[61]

For the time being, however, supporters of an American RTBF need to be creative and work within the conventional interpretation of the law to shape such a right as First Amendment-friendly. With this intent in mind, Walker proposed an interesting theory that would allow for a limited recognition of the RTBF in the United States without creating conflict with the consolidated First Amendment jurisprudence. According to his theory, "formulating data privacy in terms of implied contractual rights avoids offending the First Amendment and offers a viable (albeit partial) solution to the concerns that the right to be forgotten attempts to address. While the [European] full measure … is incompatible with American constitutional … law … a right to delete voluntarily submitted data is

[61] Pro Swing Inc. v. Elta Golf Inc., 2006 SCC 52, 1.

legally cognizable,"[62] and consistent with Warren and Brandeis's vision of the right to privacy as an implied contract.[63]

In particular, given that data privacy contracts are based on the parties' voluntary and self-imposed restrictions on their freedom of expression, there should not be any basis to validly assert that a waiver limiting such freedom would be unconstitutional on First Amendment grounds.[64] In fact, as the Supreme Court made clear in *Cohen v. Cowles Media*,[65] "[t]he parties themselves . . . determine the scope of their legal obligations, and any restrictions that may be placed on the publication of truthful information are self-imposed."[66] Therefore, a right to delete voluntarily submitted data based on self-imposed contractual terms would be consistent with the above-mentioned consolidated First Amendment caselaw and support the public's reasonable expectations of data protection, creating a *de facto* alignment with international privacy norms and improving data management technologies "without running afoul of the U.S. Constitution."[67]

However, as Walker himself points out, framing the RTBF in terms of implied contractual obligations raises the major problem of privity of contract and, in turn, lack of standing in litigation

[62] Walker, *supra* note 53, at 285. *See also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1122 (2000). ("[R]estrictions on speech that reveals personal information are constitutional under current doctrine only if they are imposed by contract, express or implied.").
[63] *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4(5) HARV. L. REV. 193, 207 (1890) ("It should be stated that, in some instances where protection has been afforded against wrongful publication, the jurisdiction has been asserted … upon the ground of an alleged breach of an implied contract or of a trust or confidence.").
[64] *See* Walker, *supra* note 53, at 283 ("Since data privacy contracts are premised on the parties' right not to speak, the government cannot mandate that an implied data deletion right is not waivable, as doing so would be state action in violation of the First Amendment.").
[65] Cohen v. Cowles Media Co., 501 U.S. 663 (1991).
[66] *See id.* at 283.
[67] *Id.* at 278.

settings.[68] For example, "a person who suffered the exposure of embarrassing personal data she did not personally disclose would not have standing for a breach of contract action against the website hosting the offending content as she is not in privity with the website nor does she benefit from the terms of service contract."[69] Therefore, the intrinsic limitations of the theory of implied contractual obligation to privacy impair its practical effectiveness.

In conclusion, Walker's theory of privacy as implied contractual obligations falls short in providing people whose private information have been exposed with a viable cause of action. Therefore, in the next section, in light of the recent Cambridge Analytica scandal and the entry into force of the General Data Protection Regulation,[70] I argue for the introduction of expressed contractual obligations in internet service providers' terms and conditions that effectively grant users a right to control their online personal information.

D. It Might be Time to Think of Online Privacy in Terms of Expressed Contractual Obligations

As observed in the preceding sections B and C, history proved that the privacy principle envisioned by Warren and Brandeis in 1890 - that an individual should be entitled to decide "whether

[68] *See* Walker, *supra* note 53, at 282 (noting the implied contract approach "is not without significant limitations. First, and most restrictive, are the requirements of contractual privity … in the United States only parties in privity to the contract have standing to enforce it. Third party beneficiaries (persons who receive some legal entitlement flowing from a contract) may have standing to sue to enforce the agreement or recover for its breach. Other parties do not.").
[69] *Id.* at 282.
[70] *See supra* note 6.

that which is his shall be given to the public"[71] - never evolved into the right to informational self-determination on which the European RTBF is founded, as observed in section A. However, the debate on the right to control online personal information is still very active. As noted by Cohen, "[b]alancing speech claims against data privacy claims also requires consideration of 'information as property'"[72] and "of both the nature of ownership and contractual interests in personally-identified information and the extent to which data privacy regulation is really directed at the exchange of information as property rather than as speech."[73]

This need to rethink the nature of online personal information has been recently emphasized by the worrisome case of Cambridge Analytica. As reported by the New York Times, private information was scraped from millions of Facebook users' profiles, adopting an approach that, according to some scientists, "could reveal more about a person than their parents or romantic partners knew."[74] Interestingly, of the more than fifty million raw profiles handed over to the firm, "[o]nly about 270,000 users … had consented to having their data harvested."[75]

[71] Warren, & Brandeis, *supra* note 63, at 199.
[72] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1420 (2000) ("Arguments from speech assume a resolution of the property question favorable to data processors, and thus no conflict between property rights and speech rights. If personally-identified data is no one's property, or property of the person who collects it, then of course this is correct. No conflict exists; to the contrary, any property interests that do exist are added to the scales on the side of (data processors') speech. But if, instead, personally-identified data is the property or quasi-property of the individual to whom it refers, then data processors' asserted speech rights cannot be absolute, and may not prevail at all.").
[73] *Id.* at 1422.
[74] Matthew Rosenberg et al., *How Trump Consultants Exploited the Facebook Data of Millions,* N.Y. TIMES (March 17, 2018), https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html.
[75] *Id.*

Commenting on the Cambridge Analytica scandal, Sally Hubbard of The Capitol Forum said "[i]t's surprising what's been permitted in terms of privacy regulations … in [the United States;] … [people] almost certainly have no idea how much Facebook knows about them and how their private data can be used in nefarious ways."[76] Indeed, it is scary to think that pieces of intimate and personal information about ourselves might be disseminated and sold without our control and authorization. This data should ultimately belong to the data subjects and not to internet service providers. In response to the widespread criticism generated by the Cambridge Analytica affair, Mark Zuckerberg recently acknowledged his "responsibility to protect [users'] data [and stated that he is] serious about doing what it takes to protect [the Facebook] community."[77]

Clearly, if the purpose moving forward is to gain people's trust in Facebook and other online service providers that collect, store and analyze our data, there is a prompt and effective solution at hand. Since "the vast majority of website terms of service agreements are 'clickwrap' adhesion contracts"[78] that users must accept without any bargaining, the best approach would be to include contractual provisions in those adhesion contracts that expressly recognize data subjects as the controller of their online personal information. This constitutionally sound contractual restriction on free speech would both create a viable and broad American RTBF and set a new standard industry practice if voluntarily followed by the most important internet service providers. For example, contractual clauses might require that after a certain amount of time from the first publication of personal information, data

[76] Sean Illing, *"It's pretty much the Wild West": why we can't trust Facebook to police itself*, VOX (March 21, 2018), https://www.vox.com/2018/3/21/17146674/facebook-cambridge-analytica-data-scandal.
[77] Mark Zuckerberg, Facebook post on March 21, 2018, available at https://www.facebook.com/zuck/posts/10104712037900071.
[78] Walker, *supra* note 53, at 283.

subjects can exercise a right to decide whether their information should remain available to the public for online consultation. This approach would safeguard both freedom of speech by allowing information to temporarily populate the online marketplace of ideas, and the individual privacy of users via a contractual right to informational self-determination that shields their reputation.

Unfortunately, however, it appears that service providers are moving in a different direction. In fact, in the midst of the entry into force of the General Data Protection Regulation,[79] Giovanni Buttarelli, the European Data Protection Supervisor, expressed general concerns about the way in which tech giants have implemented the new privacy rules.[80] In particular, Buttarelli criticized the take-it-or-leave-it approach to terms of use and conditions adopted by major service providers, which in some instances has the practical effect of blackmailing data subjects into consenting to the treatment of their data by threatening total service interruption.[81]

In conclusion, even if the path to recognition of the RTBF in the United States cannot mirror the European Union's, expressed contractual obligations may offer the first practicable, voluntary and effective step in the recognition of such right in the land of the First Amendment. This approach would protect both the online data and privacy of American people and offer online service providers an opportunity to build trust.

---

[79] *See supra* note 6.

[80] *See* Jake Kanter, *EU privacy watchdog: Big tech firms are 'blackmailing' users into agreeing with their new data terms*, BUSINESS INSIDER (May 25, 2018) http://www.businessinsider.com/giovanni-buttarelli-tech-firms-blackmail-users-gdpr-2018-5?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+typepad%2Falleyinsider%2Fsilicon_alley_insider+%28Silicon+Alley+Insider%29.

[81] *Id.* ("Buttarelli said his office will examine the 'tech giants' take-it-or-leave-it approach to data consent, which he said in some cases amounts to a 'blackmailing' of users because if they don't agree, they will be kicked off the platform.").