A CRIME REMEMBERED: THE POSSIBLE IMPACT OF THE "RIGHT TO BE FORGOTTEN" IN THE UNITED STATES FOR CRIME VICTIMS, CRIMINAL DEFENDANTS, AND THE CONVICTED

NOTE

Megan Deitz*

* JD Candidate 2018, The University of Alabama School of Law.

I. INTRODUCTION

"Search…" The dialog box awaits the command of a few keys and a click to transport the user into a cyberspace of forgotten song lyrics, current deals on electronics, or the latest news and best sellers. A jump from internet browsing to Facebook's timeline reveals a thread of friends' memes, candid photos, and posts, headed by a dialog box cheerfully asking, "What's on your mind?" Yet, for some, the cyber world of ready information and instant sharing proves a sinister resource and barrier to reintegrating into society.

A single browser search can lead the curious to mug shots, revenge porn, prior convictions, and newspaper articles of events that would preferably be left in an abandoned dark corner. In the past, few remedies existed for an individual wishing to remove public posts about himself on the internet.[1] But recently, the European Union's ("E.U.") highest judiciary created a new fundamental legal right, allowing an E.U. citizen to request that a data controller remove embarrassing search results from his name.[2] Within eight months of the ruling, the recognized "Right to be Forgotten" ("RTBF") left Google flooded with over two hundred thousand removal requests from users in the E.U.[3]

In this area of the law, the First Amendment right to free speech remains supreme after the Ninth Circuit held that the RTBF does not exist in the United States.[4] The First Amendment prohibits the restriction of citizens' speech, whether verbal or written, without a compelling government interest implemented through narrowly tailored means.[5] Acceptance of the E.U.'s proposed RTBF in the United States would create a clash between the constitutional right to free speech for an online publisher and the public

---

1. Ravi Antani, *PRIVACY LAW: Resistance to Memory: Could the European Union's Right to be Forgotten Exist in the United States,* 30 BERKELEY TECH. L.J. 1173, 1184-85 (2015).

2. Case C-131/12, Google Spain SL v. Gonzalez, 2014 E.C.R. 317, 91-94 (May 13, 2014), http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1033117.

3. *Search Removals Under European Privacy Law*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/euprivacy/overview (last visited Nov. 22, 2016). As of November 2016, the number of removal requests exceeds 630,000 complaints.

4. Garcia v. Google, Inc., 786 F.3d 733, 746 (2015) (holding that a transformed video clip of an actress' casting call would not be removed from YouTube despite death threats because there was no recognized RTBF in the United States).

5. Antani, *supra* note 1, at 1186.

versus an individual's statutory or common law privacy right to be forgotten.[6] However, compelling privacy interests exist for victims of crime who are seconds away from being re-victimized by individuals searching their names and finding the gruesome details of the acts committed against them.[7] Additionally, while former criminal defendants may have charges dropped or convictions expunged, both groups will find the internet far less forgiving, displaying their mug shots and criminal records to any online user with the right combination of search terms.[8]

This article addresses the possibility of enacting a modified RTBF in the United States, specifically tailored to victims of crimes, former defendants, and certain convicted individuals mentioned in web searches and social media. Though the right to free speech receives great deference, the privacy right to have one's personal information limited must be addressed, particularly when dealing with victims of heinous crimes or individuals whose crimes are expunged. Part I of this article examines the creation of the RTBF in the European Union and contrasts it with the limited privacy right offered in the United States. Part II discusses how the RTBF affects search engine companies and the similarities and differences between internal review of data by search engines compliant with the E.U.'s Directive and social media companies. Part III presents methods by which the RTBF could be tailored in the United States for victims, former criminal defendants, and certain convicted individuals to overcome free speech arguments.

II. THE RTBF IN THE BATTLE BETWEEN PRIVACY AND FREE SPEECH

A. Development of the RTBF

In *Google Spain v. Gonzalez*, the Court of Justice of the European Union ("Court of Justice") applied the E.U.'s Directive 95/46 to a Spanish citizen's request to Google Spain and Google, Inc. to remove web links associating his name with a public auction notice for his home after defaulting on his social security debts.[9] Directive 95/46 states that personal data processed online must be (1) "processed fairly and lawfully," (2) "collected for specified,

---

6. Edward Lee, *The Right to be Forgotten v. Right to Free Speech*, 12 J. L. & POL'Y INFO. SOC'Y 85, 93-94 (2016).

7. *Id.* at 106-09; Antani, *supra* note 1, at 1201.

8. Jessica Ronay, *Adults Post the Darndest Things: [Ctrl + Shift] Freedom of Speech to [Esc] Our Past*, 46 U. TOL. L. REV. 73 (2014).

9. *Gonzalez*, 2014 E.C.R. at 3, 14.

explicit and legitimate purposes and not further processed in a way incompatible with those purposes," (3) "adequate, relevant and not excessive in relation to purposes for which they are collected," (4) "accurate and, where necessary, kept up to date [with] every reasonable step . . . taken to ensure that data [which is] inaccurate or incomplete . . . [be] erased or rectified," and (5) "kept in a form which permits identification of data subjects *for no longer than is necessary* for the purposes for which the data were collected."[10] Responsibility for maintaining in compliance with Directive 95/46 rests entirely upon the "controller,"[11] who is the "natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data."[12]

The Court of Justice concluded that Google qualified as a controller of personal data and thus is required, upon request of an E.U. citizen, to remove information deemed "to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine."[13] The Court of Justice specifically noted that the fundamental right of an E.U. citizen to be forgotten "override[s] . . . not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information" unless the citizen was "in public life."[14] While the RTBF is not absolute in the E.U., the burden remains on the data controller to prove that its denial of a removal request was necessary to protect the public interest regarding public health, historical or scientific purposes, or legal obligations to retain the data.[15]

---

10. Directive 95/46/EC of the European Parliament and of the Council of 24 Oct. 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, ch. 2 § 1 art. 6, 1995 O.J. (L 281) 40 (emphasis added) http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.

11. *Id.* at ch. 1 art. 2 (d), http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

12. *Id.*

13. *Gonzalez*, 2014 E.C.R. at 94.

14. *Id.* at 99.

15. Ronay, *supra* note 8, at 80. Though it appears the E.U. values privacy over the public's right to information, the RTBF does not overpower a third party's ability to publish data, including an individual's personal information, as long as it is a "legitimate journalistic, literary, or artistic exercise." *Id.* at 81. Additionally, the request to remove the data is not automatically granted. Instead, the data controller reviews the request as well as a supervisory or judicial authority if the request is denied by the controller. *Gonzalez*, 2014 E.C.R. at 77.

B. The United States' Lack of Privacy Protection

In contrast to the E.U., the United States protects publishers of other individual's data with several legal theories that place heavy burdens on the subject of the data to show a compelling reason for the information's removal.[16] These heavy burdens originate primarily from the First Amendment's protection of freedom of speech from government regulation.[17] While the publishing of personal data by a third party does not involve a government entity at the outset, as soon as the dispute requires a judge to critique the content a third party posted, a restriction imposed by the government occurs.[18] Any restriction imposed on the expression of free speech must qualify as a "compelling government interest" and be narrowly tailored to carry out that interest.[19] However, successful restrictions of an individual's speech are rare because the narrowly tailored regulation must be the "least restrictive alternative that can be used to achieve that goal."[20] Thus,

16. Ronay, *supra* note 8, at 87 (noting that generally a data subject must contact the host search engine themselves to plead their case and establish that the content violates the server's terms).

17. U.S. CONST. amend. I.

18. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 265 (1964) (holding that disputes of a civil action do not matter nor the form of state power applied but "whether such power has in fact been exercised" by the court making a judgment and thus a regulation by the government concerning a matter of speech); Antani, *supra* note 1, at 1185-86 (noting the impact of *Sullivan* and the existence of "state action" by a court's judgment on the statements of a private party).

19. Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 741 (1996) (explaining that the government "may directly regulate speech to address extraordinary problems, where its regulations are appropriately tailored to resolve those problems without imposing an unnecessarily great restriction on speech"); Sable Comm'n Cal. v. FCC, 492 U.S. 115, 126 (1989) (noting that the government's legitimate interest must be enacted through "narrowly drawn regulations" to avoid triggering the prohibitions of the First Amendment); First Nat'l Bank v. Bellotti, 435 U.S. 765, 786 (1978) (concluding that the government may prevail [if they] can show a compelling interest).

20. Ashcroft v. ACLU, 542 U.S. 656, 666 (2004) (finding that the Child Online Protection Act violated the First Amendment, because criminalizing the posting of information "harmful to children" was not the least restrictive method to protect children from obscene or offensive content); *see also* Reno v. ACLU, 521 U.S. 844 (holding that the Communications Decency Act of 1996, penalizing the sending of obscene and offensive messages to children under the age of 18, was an

states are prohibited from passing laws restricting the media from portraying truthful information however a specific media organization sees fit, regardless of whether the idea portrayed is distasteful to society.[21]

Additionally, civil actions, such as claims for defamation, breach of contract, and privacy torts, have little if any effect on limiting the spread of personal information.[22] Yet, the revered principle of free speech does not diminish the effect of personally damaging information floating around the internet without restraint.[23] An examination of a tailored RTBF in the United States through data controllers could serve as the compromise between free speech and privacy where other legal remedies have failed.

III. THE RTBF'S EFFECT ON DATA CONTROLLERS

The *Gonzalez* decision defined data controllers as a body or person who controlled the purpose and use of personal data.[24] Since Google Spain, as a search engine, determined how and what activity would be performed through its service, the Court of Justice concluded that Google Spain and, logically, all other search engines were data controllers.[25] Similarly, social media websites operate under various rules agreed to by their users that govern the use of personal data on the site,[26] likely making them data controllers.

---

unacceptable statute, because less restrictive measures to achieve the regulation's purpose existed).

21. *See* Smith v. Daily Mail Publishing Co., 443 U.S. 97, 106 (holding that punishing a newspaper for accurately printing the name of a juvenile delinquent was unconstitutional when the name was legally obtained); Antani, *supra* note 1, at 1186.

22. Ronay, *supra* note 8, at 87. Defamation only removes false information pertaining to a non-public figure but not embarrassing, harassing, or offensive content. Breach of contract claims only inhibit the parties to the contract from sharing information but not any other persons or entities that the information has already reached through one of the breaching parties or another source. Finally, privacy torts fall short of protecting an individual's privacy if the subject has already shared the information but then seeks to withdraw the information after the information becomes viral. *Id.* at 87-88.

23. Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES (July 21, 2010) (detailing how information posted to the internet continues to morph as it is shared to multiple other sites making the data last forever).

24. *Gonzalez*, 2014 E.C.R. at 32.

25. *Id.* at 33.

26. See, *Facebook Terms and Policies*, FACEBOOK, www.facebook.com/policies (last visited Oct. 08, 2017); *Data Policy*, FACEBOOK, www.facebook.com/about/privacy (last visited Oct. 08, 2017); *Twitter Privacy Policy*, TWITTER, www.twitter.com/privacy (last visited Oct. 08, 2017).

A. Search Engines

Subsequent to the Court of Justice's ruling, Google, Inc. provided a web form to E.U. users that allowed them to request the removal of URLs they felt violated their privacy, to be submitted for internal company review.[27] If upon review the link is found to violate the Directive, Google sends a voluntary notice to the publisher that the link to its post has been removed from the search page of the individual's name, even though *Gonzalez* does not require notice to be given to the publisher.[28] Yet, the removal of links associated with an individual's name only occurs on the domain of the country the user requests, not across all E.U. or worldwide domains.[29]

Regardless, Google's in-house resolution regarding removal requests from specific domains in the E.U. suggests a means of acceptance of the RTBF in the United States. The First Amendment prohibits the government's interference with a citizen's right to free speech, but does not prohibit private actors from limiting free speech unless a court rules on the interference.[30] Thus, private companies have an opportunity to resolve conflicts arising from undesirable or embarrassing data. For example, many news sources have adopted voluntary rape shield policies that report the facts of the crime but do not supply the name of the victim.[31] Or, like Google Spain, private companies may internally review complaints from subjects of data content.

An adoption by private companies in America of internal reviews similar to what already takes place in Google's E.U. forum would provide some protection to the data subject, rather than having information immediately available about him from a simple search.[32] The review could adopt similar principles as seen in the *Gonzalez* decision, weighing the relevance and date of the content versus the public, historical, or legal interest associated with the information.[33] Notably, a final decision to remove a search result does not have to remove the publisher's content but could simply delete the content's association with data subjects from internet queries of their names.[34]

---

27. Antani, *supra* note 1, at 1180; *see E.U. Privacy*, GOOGLE, https://www.google.com/webmasters/tools/legal-removal-request?complaint_type=rtbf&visit_id=0-636386964994598184-1168322459&rd=1# (last visited August 18, 2017).
28. Antani, *supra* note 1, at 1180.
29. I*d.* at 1178.
30. Antani, *supra* note 1, at 1185-86.
31. Lee, *supra* note 6, at 104.
32. *Id.* at 103.
33. *Id.*
34. *Id*. at 105.

Internal decision making raises some concerns about placing the publisher and the public's right to free speech in the hands of a private company.[35] However, post *Gonzalez*, Google continues to handle removal requests internally, granting removal to 43.2% of complaints, with review by a data protection agency occurring only upon protest.[36] An internal review is already in place in many online services, especially social media platforms, for content that offends community guidelines, justifying complete content removal by the platform service.[37] In contrast, the RTBF review implemented by Google does not delete content, but instead removes search result links to offensive content about a data user, effectively hiding information from all but the extremely persistent rather than destroying the data altogether.[38]

An alternative solution exists in filtering search links rather than completely removing them. The introduction of a filtering algorithm would begin to "derank" search results from a person's name over time once a complaint is lodged and approved.[39] A progressive deranking of offensive search results over the passage of time would protect the right to free speech while maintaining an individual's privacy from the general population.[40] The deranking could be managed by the search engine provider, rather than placing it in the hands of high priced companies offering similar services by flooding the internet with positive data about individuals to push negative results to back pages.[41] This would create a balance between free speech and privacy to remain as the data controller weighs the relevance of the content against the public's interest in the information, similar to Google Spain's internal review, rather than weighing a large price tag of profit. The internet's endless storage of information creates a need for either a removal or deranking of search results to protect a crime victim's privacy and guard acquitted defendants or convicted individuals from discrimination.

---

35. *Id.* at 103.

36. Transparency Report, *supra* note 3.

37. Antani, *supra* note 1, at 1204. *See Facebook Community Standards*, FACEBOOK, https://www.facebook.com/communitystandards (last visited Aug. 18, 2017); *The Twitter Rules*, TWITTER, https://support.twitter.com/articles/18311 (last visited Aug. 18, 2017).

38. Antani, *supra* note 1, at 1179-1180.

39. Lee, *supra* note 6, at 105-06.

40. *Id.*

41. REPUTATIONDEFENDER, https://www.reputationdefender.com/reputation (last visited Nov. 24, 2016); GURANTEEDRESULTS.COM, http://guaranteedremovals.com/push-down-complaints/ (last visited Nov. 24, 2016).

B. Social Media

Search result removal or deranking of search results by a search engine is a tamer version of the data control procedures exercised by social media sites regarding users' posted content. On social media, threats to personal privacy come from two main sources, the individual user and fellow users she is "friends" with.[42] An individual is free to post any content that abides by the website's community guidelines, whether the information discusses her or others.[43] Once posted, that individual's friends are free to share the post with their friends into an infinity of viral sharing.[44] Upon signing up for a profile on a social media site, users are confronted with privacy notices that they must consent to in order to complete their registration.[45] User uploaded information is not considered secret or private once shared on the social media site, as all copyrights are signed over to the online platform upon agreeing to the site's terms and conditions.[46]

However, protections are also afforded to platform users based upon the agreed community terms and conditions.[47] Companies like Facebook, Twitter, and Instagram accept reports of inappropriate content containing bullying, harassment, criminal activity, abuse, nudity, or the posting of private information, such as addresses and Social Security numbers, without permission.[48] Upon internal review, the company is free to take action, ranging from removing a post to permanently suspending a user due to inappropriate content.[49] Thus, social media companies are already taking steps similar to the RTBF to protect the user's privacy, because users have consented to have their right to free speech limited within the community.[50] Yet, unless search engines also begin to require users to sign an agreement before utilizing the service, a balance between the complete removal of content by social media sites and the complete lack of privacy on search

---

42. Lothar Determann, *Social Media Privacy: A Dozen Myths and Facts*, 2012 STAN. TECH. L. REV. 7, 3 (2012).

43. *Id*.

44. *Id.*

45. *Id.* at 5.

46. *Id.* at 6.

47. *Id*. at 2.

48. *See Facebook Community Standards*, *supra* note 34; *The Twitter Rules*, *supra* note 34; *Community Guidelines*, INSTAGRAM, https://help.instagram.com/477434105621119 (last visited Aug. 18, 2017).

49. *Id.*

50. Determann, *supra* note 33, at 14.

engines becomes essential as internet users continue to share information without any inhibition.[51]

IV. RTBF'S IMPACT ON CRIMINAL JUSTICE

For individuals involved in the criminal justice system, an interesting duel exists between the individual's RTBF and the community's interest in being informed to maintain public safety. While an unlimited RTBF could threaten public wellbeing, a tailored RTBF made available to crime victims, former criminal defendants, and certain convicted individuals protects those whose circumstances subject them to unnecessary prejudice and punishment.

A. Criminal Victims

For a crime victim, the RTBF presents an opportunity to forget some of the worst memories of her life. Often facts about a victim's rape or kidnapping are available to any internet user that runs a search of the victim's name, since news outlets are not legally limited in what facts they report.[52] For one victim, information and testimony she gave concerning her childhood rape can be found on the first page of Google search results of her name twenty years later.[53] Meanwhile, a family receives little comfort knowing that the public can run a search for "decapitated girl" and find graphic pictures of their daughter's body.[54] Victims of revenge porn, sexual photographs or videos posted without their consent, are just beginning to receive a criminal remedy in thirty-eight states, plus D.C., through the prosecution of the posting individual.[55] However, in the remaining states, if the content does not

51. *Id*.

52. Lee, *supra* note 6, at 108.

53. *Id*. at 109. Kiri Jewell testified before Congress about her rape as a child by cult leader David Koresh.

54. Jeffrey Toobin, *The Solace of Oblivion: In Europe, The Right to be Forgotten Trumps the Internet*, NEW YORKER (Sept. 29, 2014). Photos of a horrific car accident showing a decapitated teenager spread across the internet from leaked police photos. The family could only stop the spreading of pictures by requesting over 2,000 individual websites to take down the pictures voluntarily. However, pictures can still be found, suggesting a similar outcome for gruesome crime photos of victims that make their way to the public. The only remedy available is reliance on the mercy of the publisher to remove the offensive content voluntarily or for profit.

55. *34 States + DC Have Revenge Porn Laws*, CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/revenge-porn-laws/(last visited Nov. 24, 2016) (listing the states with current revenge porn laws and providing links to the respective statute).

contain child pornography or violate state stalking laws, the victim is limited to voluntary removal by the publisher since pornography, consensual or not, is still considered a form of free speech.[56]

Regardless of whether content is posted on social media or a website linked to a search engine, victims are currently limited to private company review and intervention, if private companies will even assist them at all. Social media sites currently remove content containing harassment or graphic content when reported[57] and Google has recently adopted a policy to remove links to revenge porn.[58] However, particularly for victims, internal company review is a treatment with a Band-Aid without additional measures in place, as the information has frequently already been shared on other platforms. Following the recent wave of legislation creating criminal punishment for revenge porn,[59] a statutory adoption of the RTBF by the United States in reference to crime victims is a possible compromise between the right to free speech and right to privacy.[60] As seen in revenge porn legislation, the right to privacy of the crime victim from offensive involuntary content overrules the right to free speech of the publisher based on a compelling government interest, the protection of victims.[61] Narrow statutes that allow for the removal of graphic or offensive content concerning a crime victim from a search engine, with subsequent judicial or agency review, offer an opportunity to enact features of the E.U.'s RTBF in the United States for other issues beyond revenge porn.[62]

---

56. Ronay, *supra* note 8, at 82.

57. *See Facebook Community Standards*, *supra* note 34; *The Twitter Rules*, *supra* note 34; *Community Guidelines*, *supra* note 42.

58. Amit Singhal, *"Revenge Porn" and Search*, GOOGLE PUBLIC POLICY BLOG (June 19, 2015), https://publicpolicy.googleblog.com/2015/06/revenge-porn-and-search.html.

59. *See e.g.*, W. Va. Code § 61-8-28a (1931) (effective July 7th, 2017) (criminalizing disclosure of private intimate images).

60. Danielle Citron, *Debunking the First Amendment Myths Surrounding Revenge Porn Laws*, FORBES (April 18, 2014); Danielle Citron, *How to Make Revenge Porn a Crime*, SLATE (Nov. 7, 2013).

61. *Id.*

62. Similar to the E.U., a court or agency could be tasked with reviewing complaints regarding internal review. Those concerned about mass requests for appealed deletion should note the low volume of cases in the E.U. that make it to an appeal stage. *See* Gonzalez, 2014 E.C.R. at 94.

B. Former Criminal Defendants

After arrest, a criminal defendant, regardless of dropped charges or acquittal, lives with the knowledge that his mug shot is one web search away from the general public.[63] While the public has a right to be informed, the presence of information on the internet and social media regarding criminal activity affects the former defendant's ability to rehabilitate through employment or educational opportunities due to prejudice and bias.[64] Currently, defendants can only remove their encounter with law enforcement from the internet through request or by paying individual companies to remove content.[65] Companies publishing mug shot photos normally only remove posts if the subject pays to have the picture removed.[66] However, payment to one website does not remove the post from another website that shared the same picture.[67] Sharing to additional sites requires the subject to pay or request each individual website to delete the mugshot.[68]

Beyond mugshots, many background check websites do not update information regularly to reflect expunged records, allowing searches of the individual's name to bring up old websites with information concerning an individual's arrest.[69] Under the Fair Credit Reporting Act, background check companies are free to report to employers any applicant's arrest, regardless of disposition, within the past seven years.[70] The EEOC instructs employers that an arrest record alone should not be used to dismiss job applicants, due to the disparate impact on protected classes.[71] But employers "may make an employment decision based on the conduct underlying the arrest if the conduct makes the individual unfit for the position in question."[72] Based on this broad grant, an employer could justify its rejection of an applicant whose charges were dropped or who obtained an acquittal on grounds that the

63. Ronay, *supra* note 8, at 84.

64. Editorial Board, *How to Get Around a Criminal Record*, N.Y. TIMES (Oct. 19, 2015); Adam Liptak, *Expunged Criminal Records Live to Tell Tales*, N.Y. TIMES (Oct. 17, 2006).

65. Ronay, *supra* note 8, at 84.

66. *Id*.

67. *Id*.

68. *Id*.

69. Editorial Board, *supra* note 64.

70. James Jacobs, *Employment Discrimination Based on Previous Arrests*, WASH. POST (Feb. 4, 2015).

71. U.S. EQUAL EMP. OPPORTUNITY COMM'N, CONSIDERATION OF ARREST AND CONVICTION RECORDS IN EMPLOYMENT DECISIONS UNDER TITLE VII OF THE CIVIL RIGHTS ACT OF 1964 (Apr. 2012), https://www.eeoc.gov/laws/guidance/arrest_conviction.cfm.

72. *Id*.

individual's alleged conduct creates concern about the applicant's performance in the open position.[73] In addition, many individuals with arrest records may experience difficulty in obtaining housing due to prejudices on the part of the landlord.[74]

While legislatures and the courts attempt to punish the discriminatory use of arrest records, limiting access to the online information concerning the arrest could prove more efficient. Even with state legislation present to erase an arrest record upon acquittal or dismissal, one former criminal defendant found that her reported arrest would continue to haunt her online after the Second Circuit ruled that she could not bring an action against any of the news sources that published an online article about her arrest.[75] Some states are attempting to move from creating statues of legal fiction to granting individuals a RTBF with legislation requiring removal of mug shots of acquitted defendants and deleting content posted by minors.[76] Even where content could not be completely deleted, preventing the information from linking to the former defendant's name would decrease prejudice. Though RTBF legislation would technically limit the availability of truthful information concerning former arrests, the "truth" of an arrest tends to produce punishments outside of the legal system that individuals who are determined not guilty are still forced to pay.

C. Convicted Individuals

In contrast, those convicted of crimes cannot expect the same protection from the RTBF as could be afforded to victims or the acquitted, because of the public's legitimate interest in being informed about their offenses against the community.[77] However, some protection of the RTBF could be provided to certain convicted individuals who qualify for the rehabilitative devices of

---

73. *See* Jacobs, *supra* note 70.

74. Camila Domonoske, *Denying Housing Over Criminal Record May Be Discrimination, Feds Say*, NAT'L PUB. RADIO (Apr. 4, 2016).

75. *See* Martin v. Hearst Corp., 777 F.3d 546, 551-52 (2d Cir. 2015) (concluding that even though the Erasure Statute created a legal determination that the plaintiff had never been arrested, it could not alter the public record).

76. Mark Joseph Stern, *Forget Me Not: A Federal Court Considers Whether We Have the Right to Tell the Truth*, SLATE (Jan. 29, 2015), http://www.slate.com /articles/technology/future_tense/2015/01/right_to_be_forgotten_do_we_have _a_first_amendment_right_to_the_truth.html.

77. Antani, *supra* note 1, at 1196-97; Ronay, *supra* note 8, at 85.

legal forgiveness or expungement of minor criminal offenses in the courts.[78] Currently, even for individuals who receive legal forgiveness or expungement, rehabilitation remains ineffective because information about their offense is still available on the internet for third parties to digest.[79] The use of a modified RTBF for non-violent misdemeanors would afford criminal defendants whose records are expunged an opportunity to reenter society without society's bias towards their recompensed criminal activity.[80]

Naturally, concerns about implementing the RTBF regarding criminal activity exist, particularly in reference to government investigations of criminal activity posted on social media or other sites on the internet.[81] However, this article's proposed use of the RTBF is narrowed to post-acquittal or post-conviction treatment of misdemeanors, because criminal activity shared online pre-conviction is important to both the government and even the defendant.[82] A narrowed RTBF should only be enjoyed by individuals who were acquitted, received forgiveness from the courts to aid in their reentry into society, or committed minor misdemeanor offenses that were not a threat to public safety.[83]

Alternatively, a deranking algorithm reducing search results over time initiated by a main search engine, like Google, would also reduce the exposure of the convicted. Similar independent services already exist, advertising a "filtering service" that reorders negative news and images from search results of an individual's name for prices ranging from three thousand to twenty-five thousand dollars.[84] However, this reordering solution limits

78. Editorial Board, *supra* note 64; Liptak, *supra* note 64.

79. I*d.*

80. Lee, *supra* note 6, at 106.

81. Determann, *supra* note 42, at 16.

82. *See* Justin P. Murphy, et. al, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 11, 5 (2013). The government is free to investigate public social media posts without a warrant, access private posts through a fake online identity the suspect "friended," or through cooperation of one of the suspect's current "friends" on social media. *Id.* at 7-8. However, defendants have a harder time obtaining evidence from social media websites as ethical rules bar defense attorneys from employing the same methods as the government and require them to subpoena the company for the records themselves. *Id.* at 21. An application of the RTBF to remove criminal activity posted by or about a user would hinder government investigations and might even hinder a defendant's ability to present another suspect, because someone could request the information be removed to keep them from being impeached or held liable.

83. Lee, *supra* note 6, at 105-07; Antani, *supra* note 1, at 1196-97.

84. Reputation Defender, https://www.reputationdefender.com/reputation (last visited Nov. 24, 2016); GuaranteedResults.com, http://guaranteedremovals.

privacy to wealthy convicted individuals. In contrast, this service can be obtained in the E.U. for free and can include the complete removal of content. Even for individuals who pay for these expensive services, background check websites often contain information concerning expunged criminal records that would not be affected by a RTBF algorithm requiring specific legislation mandating that companies keep their data up to date.[85]

V. CONCLUSION

A multi-front intervention is necessary. Legislation enacting the RTBF for victims through the removal of search results while allowing publishers to keep content provides some protection. In contrast, former criminal defendants or individuals convicted of misdemeanors could utilize a deranking algorithm provided upon request by the search engine based on a created set of conditions, such as that the crime be non-violent, as a RTBF remedy possible in the United States.[86] For expunged crimes, a RTBF remedy should be provided by the court to expunge the crime from both the individual's legal record and remove search links to information concerning the arrest. Legislation should be enacted requiring background check sites to remove expunged information as well as dismissed arrests and requiring sites keep their data up to date. Any free speech claim presented by a news or background check website would already be hindered since, upon granting expungement, the court decided that the public did not have a "legal" right to know about the criminal record and because the association is what is deleted, not the host's content.[87]

The preceding arguments are only a few options offered to combat the privacy issues faced by crime victims, former criminal defendants, and convicted individuals by adopting a modified RTBF. Victims deserve an opportunity to forget the atrocities committed against them and avoid continued invasions into their privacy. The RTBF serves as an available tool to make that happen in the context of growing online information.[88]

For former criminal defendants and convicted individuals, unemployment and other prejudices created by their past criminal record could be prevented to some degree by the adoption of the RTBF or a

---

com/push-down-complaints/ (last visited Nov. 24, 2016).

85. Liptak, *supra* note 64.

86. Lee, *supra* note 6, at 105-07; Antani, *supra* note 1, at 1196-97.

87. *See* Editorial Board, *supra* note 64; Liptak, *supra* note 64.

88. Lee, *supra* note 6, at 108.

deranking RTBF algorithm, slowly reducing the prominence of the information over time.[89] While our country embraces a dedication to free speech, the United States also recognizes a right to privacy that is currently inapplicable to the largest information provider on the planet, the internet. For individuals exposed to the criminal justice system, the only information forgotten on the internet is their privacy. Privacy that could be rebuilt by recognition of the RTBF in the United States.

89. Antani, *supra* note 1, at 1197.