IP Theory

Volume 2 | Issue 2 Article 5

Winter 2012

The End of Forgetting and "Administrative Rights" to Our Online Personas

Jamie R. Lund
Saint Mary's University School of Law, San Antonio, Texas, jlund1@stmarytx.edu

IPtheory Volume 2: Issue 2

The End of Forgetting and "Administrative Rights" to Our Online Personas

Jamie R. Lund*

Introduction

In Jorge Luis Borges short story, *Funes el Memorioso*, the titular Funes suffers a brain injury that results in an inability to forget.[1] At first his altered status feels more gift than impairment. He is capable of fantastic mental feats. He no longer wastes time trying to learn things by repetition. Every important detail is immediately accessible to his extraordinary brain, allowing him to spend less time on drudgery. He is also able to focus and remember minutiae like he was never capable of before. The world unfolds before him in striking clarity. No data point, however inconsequential, escapes his viselike attention to detail. Alas, this becomes his downfall. He loses focus on the important. Not forced to prioritize on initial intake due to a limited storage capacity, he drowns in a sea of the irrelevant.[2]

In his New York Times piece, "The Web Means the End of Forgetting," legal commentator Jeffrey Rosen warns of the special problem the web presents, particularly for people's personal lives.[3] Rosen warns: "we are only beginning to understand the costs of an age in which so much of what we say, and of what others say about us, goes into our permanent — and public — digital files."[4]

Although new tools like Google's "Me on the Web" are allowing users to better monitor their personal information available on the web, there is no real means of managing this information. This article seeks to explore what it would take to have enforceable "administrative rights" to one's personal information – the ability to edit or modify one's online persona just as a webmaster would be able to edit or modify on an individual

---

† Assistant Professor of Law, Saint Mary's University School of Law. Special thanks to my research assistants Clark Swenson, Amy Zetzman, Michel Butler, and Stephen Vogel for their excellent editorial and research support.

1. Jorge L. Borges, *Funes the Memorious*, *in* Ficciones 107-15 (Anthony Kerrigan & Anthony Bonner eds., 1962).
2. *Id.*
3. Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. Times, Jul. 21, 2010, at MM30.
4. *Id.*

website.[5] This article first explores the inadequacy of extra-legal means available for monitoring one's online persona, concluding that these means are insufficient. It then gives an overview of legal hurdles to managing one's personal information online and suggests some possible legal solutions to the "end of forgetting," including the European Union's recently proposed new privacy policies, including a "right to be forgotten," or a possible property right in one's readily identifiable personal information.

I. Non-legal Options for Monitoring One's Online Persona

The growth of social networking and mobile communication technology has led to increasing concerns about control of personal information online. Only a decade or so ago, it was somewhat of a fad for individuals to "Google" themselves to see what the search engine managed to pick up. Now many do not bother monitoring their online persona at all. On the contrary, through social networking, users happily volunteer huge amounts of personal information for all eyes to see, including advertisers, hackers, identity thieves, and personal and business contacts.[6] Many have found out the hard way that failure to manage their online personas can lead to negative outcomes in real life.[7]

A. Efforts to Educate Web Users About Online Privacy Management

The web is becoming an increasingly risky place for the average user, as shown by many recent efforts to protect privacy through legislation and efforts to educate individuals on how they can manage their online identities.[8] Among these efforts is Onguard.com, a

---

5. According to an Indiana University Information Technology website:

> An administrator is a local account or a local security group with complete and unrestricted access to create, delete, and modify files, folders, and settings on a particular computer. This is in contrast to other types of user accounts that have been granted only specific permissions and levels of access. An administrator account is used to make systemwide changes to the computer, such as:
>
> - Creating or deleting user accounts on the computer Creating account passwords for other users on the computer Changing others' account names, pictures, passwords, and types
> - Administrative rights are permissions granted by administrators to users allowing them to make such changes.
>
> Without administrative rights, you cannot perform many such system modifications, including installing software or changing network settings.

On a Computer, What Are Administrators and Administrative Rights, Ind. Univ. Univ. Info. Tech. Servs. (last modified Mar. 31, 2010), http://kb.iu.edu/data/aorq.html.

6. The information available through our web identity poses risks to our reputation, allows hackers and criminals to steal or use our identities, and leads to "relevant" (or creepy) ads that follow us around as we surf the web. Understandably, there is no shortage of efforts to keep our web identities private.

7. Rosen, *supra* note 3. Among other victims of "the end of forgetting," the author tells the story of Stacy Snyder, a 25-year-old studying to be a teacher who was denied her degree due to some old, but unbecoming, MySpace photos of her drunk, decked out in a pirate hat.

8. Keir Thomas, *Google's 'Me on the Web' Tool Alerts You to Personal Data Leaks*, PC World (June 16, 2011 8:01am), http://www.pcworld.com/printable/article/id,230436/printable.html.

Federal site run by the FTC that broadly seeks to educate and inform the public on how to protect their online identities.[9] StopBadware is a prevention, mediation, and remediation organization that is more protective in nature, acting as a sort of law enforcement against sites with viruses, spyware, scareware, and other badware.[10] The National Cyber Security Alliance focuses on awareness of the privacy problem, and is one of the initiators of National Cyber Security Awareness Month (October).[11] The movement's message campaign "Stop. Think. Connect." is a collaborative effort, managed by the Department of Homeland Security, which aims to do what "Smokey Bear" did for forest fire safety, or what "Click It or Ticket" did for seatbelt safety.[12] On January 17, 2012,[13] Google launched a similar campaign called "Good to Know," aiming to make online safety and identity management user-friendly.[14]

Google's recent "Me on the Web" takes such efforts at education a step forward and attempts to not just inform users about their online presence, but to actually allow Google users to monitor it themselves.

B. Google's Me on the Web Allows for Monitoring but Not Correction or Management of Online Identities

"Me on the Web" allows Google users to monitor when their name, email account, or other personal information is posted online, including on social networking sites (including being identified or "tagged" in pictures), blogs, and news posts.[15] It uses an email notification system to alert the user when such information is posted on the web, which users can set to receive instantly, weekly, or monthly.[16] Me on the Web can even suggest certain keywords to monitor activity that may be linked to your identity.[17] Me on the Web will not, however, allow users to control any of this information, it only provides references that may help remove or manage unwanted browsing history information.[18]

---

9. *About Us*, OnGuardOnline.gov, http://onguardonline.gov/about-us.
10. *About StopBadware*, StopBadware, http://www.stopbadware.org/home/about.
11. *About the National Cyber Security Alliance*, Nat'l Cyber Security Alliance, http://www.staysafeonline.org/about-us/about-national-cyber-security-alliance.
12. *Partners and Resources*, Google, http://www.google.com/goodtoknow/partners/; *Welcome*, Stop Think Connect, http://stopthinkconnect.org/.
13. Clint Boulton, *Google 'Good to Know' Campaign Touts Web Privacy, Security*, eWeek.com (Jan. 17, 2012) http://www.eweek.com/c/a/Security/Google-Good-to-Know-Campaign-Touts-Web-Privacy-Security-706900/.
14. *The Good to Know Campaign*, Google, http://www.google.com/goodtoknow/campaign/.
15. Simon Gould ("The Blue Guy"), *Google Me on the Web–And What You Need to Know*, Inform Digital Marketing (Feb. 29, 2012) http://www.informdigital.com/stayinformd/index.php/google-me-on-the-web.
16. Thomas, *supra* note 8.
17. Andreas Tuerk, *Me, Myself and I: Helping to Manage Your Identity on the Web*, Google Public Policy Blog (June 15, 2011, 1:30 PM), http://googlepublicpolicy.blogspot.com/2011/06/me-myself-and-i-helping-to-manage-your.html.
18. Gould, *supra* note 15.

Prior to Me on the Web, Google's Dashboard already had an alert tool available for Google account holders, but it was arguably not as user-friendly.[19] Me on the Web is arranged so users can see, manage, and fix problems in one place,[20] although Me on the Web users will only see information from sites that they have linked to their Google account.[21] The "helpful" resources are also limited, as there is little you can do to remove information posted by others' sites.[22] Probably the biggest limitation, though, is that you must create a Google account to gain access to the Dashboard.[23]

Many people show doubt in the real purpose behind Me on the Web. A few see it as an opportunity to combat online vigilantism.[24] Me on the Web may be a direct response to allegations made by Facebook against Google, claiming that Google was secretly collecting information from Facebook without people's knowledge or permission.[25] Others see Me on the Web as a ploy to get Google into the social game.[26] When you create a Google user account, you are automatically enrolled in Google+, which is Google's social networking site.[27] Furthermore, creating an account only creates more opportunities for collecting personal information.[28] Overall, Google's Me on the Web is a somewhat useful, yet a notably redundant way to get users to take action in managing their online reputation.

---

19. Tuerk, *supra* note 17.
20. Danny Sullivan, *Google's "Me on the Web" Pushes Google Profiles—Take That, Facebook?*, Search Engine Land (June 15, 2011, 7:57 PM), http://searchengineland.com/google-me-on-the-web-pushes-google-profiles-81874.
21. *Id*. These might include Yahoo, Facebook, or other sites with profiles that allow linking to a Google account.
22. *Id*.
23. *See* Monique Neeley, *What Is "Me on the Web"*, My Digital World (June 18, 2011), http://moniqueneeley.com/?p=1058.
24. Thomas, *supra* note 8.
25. Sullivan, *supra* note 20.
26. Neeley, *supra* note 23; Alexis Madrigal, *I'm Being Followed: How Google–and 104 Other Companies–Track Me on the Web*, The Atlantic / Nat'l J. (Mar. 1, 2012), http://nationaljournal.com/tech/i-m-being-followed-how-google-and-104-other-companies-track-me-on-the-web-20120301.
27. Google+, or G+, was launched last year, and was Google's fourth attempt at competing with Facebook. As of December 2011, G+ was adding around 625,000 new users a day. It now has close to 100 million; Facebook has 900 million. For more information on G+, see Martin Kaste, *Facebook's Newest Challenger: Google+*, NPR (June 29, 2011), http://www.npr.org/2011/06/29/137507567/facebooks-newest-challenger-google-plus; Matthew Shaer, *Looking for a Google+ Invite? Either Get Comfortable–or Get Crafty*, The Christian Science Monitor (June 30, 2011), http://www.csmonitor.com/Innovation/Horizons/2011/0630/Looking-for-a-Google-invite-Either-get-comfortable-or-get-crafty.; Paul Boutin, *Google+ for Everyone—What You Need To Know*, N.Y. Times (Sept. 20, 2011), http://gadgetwise.blogs.nytimes.com/2011/09/20/google-for-everyone-what-you-need-to-know/; Claire Cain Miller, *Another Try by Google to Take on Facebook*, N.Y. Times (June 28, 2011), http://www.nytimes.com/2011/06/29/technology/29google.html&pagewanted=all; Lucas Shaw, *Google 4Q Earnings Miss the Mark, Google Plus Hits 90M Subs*, Reuters (Jan. 19, 2011), http://www.reuters.com/article/2012/01/19/idUS427563801220120119; Jessica Guynn, *Google+ May Reach 400 Million Users by End of 2012*, L.A. Times (Dec. 27, 2011), http://latimesblogs.latimes.com/technology/2011/12/google-may-reach-400-million-users-by-end-of-2012.html.
28. Sullivan, *supra* note 20.

C. Google's New Policies Regarding Personal Information Suggests Further Incursions on Web Privacy Without Any Accompanying Ability to Opt Out or Otherwise Manage the Use of Personal Information

Two new changes for Google represent a big shift for Google users in terms of how their personal information is used. First, on January 10, 2012, Google launched "Search Plus Your World," which accesses users' personal information from all of their Google accounts in conjunction with Google's regular search engine to give users a much more personalized list of results.[29] Second, on March 1, 2012 Google's new unified privacy policy became effective, allowing Google to combine all information that it collects regarding its users into one data set under the user's individual Google profile name.[30] For Google account holders, this includes name, email address, Gmail message content, and any other information provided in obtaining the account.[31] The effect is to give advertisers a more cohesive collection of information for targeted advertising.[32] This nice collection of information will also be visible to any diligent hacker,[33] and there is no option to opt-out of this new system.[34]

This is unprecedented. Previously, Google separately collected two types of information: (1) information connected to individual names regardless of the computer used ("identity-linked information") and (2) information related to our internet habits, which is determined by the computer used and is used by advertisers to personalize ads based on the computer's search history ("browsing history information").[35] Regarding the latter information, one journalist reported that 105 companies, including Google, tracked her web movements over a 36-hour period.[36] When she tried using Mozilla's "Collusion" and using an "Opt Out" form, she realized that she could never stop data collecting; the best she could do was limit some of the information gathered from being used by the companies.[37] Google's Dashboard does not give users access to

---

29. Miranda Miller, *Google Launches Search Plus Your World*, Search Engine Watch (Jan. 10, 2012), http://searchenginewatch.com/article/2136615/Google-Launches-Search-Plus-Your-World.
30. Julie Sartain, *6 Things You Need to Know About Google's New Privacy Policy*, Network World (Feb. 27, 2012, 6:00 AM), http://www.networkworld.com/news/2012/022712-google-privacy-policy-256399.html. Before March 1, Google had around 70 different privacy policies. Dwight Silverman, *Google's New Privacy Policy Takes Effect Today. Does it Really Matter?*, Chron.com (Mar. 1, 2012), http://blog.chron.com/techblog/2012/03/googles-new-privacy-policy-takes-effect-today-does-it-really-matter/.
31. *See* Sartain, *supra* note 30; Silverman, *supra* note 30.
32. Sartain, *supra* note 30.
33. Those who use sites like Google, Twitter, and Facebook have the highest incidence of fraud. *See* Michelle Singletary, *Color of Money: Protect Your Identity*, BlackAmericaWeb.com (Feb. 28, 2012, 5:27 PM), http://www.blackamericaweb.com/?q=articles/money/personal_finance_money/37561. When you set up a Google account, you are immediately encouraged to link these sites with your Google account.
34. Sartain, *supra* note 30.
35. Madrigal, *supra* note 26.
36. *Id.*
37. *Id.*

server logs, cookies, and information used for internet-based advertising,[38] however Google traditionally kept this information separate from information unique to a personal name or profile to protect Google account holders.[39] Google's new approach to information management combines these two types of information "in a single dossier."[40]

Google's Policy Manager claims, "Our privacy controls have not changed. Period."[41] Technically, that is true, because Google has been collecting the same data to sell to advertisers since 2004, only spread across 70 different privacy policies[42] for each of Google's products.[43] If you are not signed into your Google account, all Google will get is identity-linked information. But, if you are signed into your Google account, not only does Google still collect the same identity-linked data, it links your profile to the huge amount of information collected based on your browsing history.

Federal regulators, along with trade groups and technology companies, met earlier this year in an attempted to thwart such policies with the "Do Not Track" initiative, which will give consumers more control over what personal information is collected online, and place limits on information collected.[44] Similarly, European Union regulators asked Google to postpone the release date in order to investigate suspicions that it violated EU law.[45] Currently, however, "Do Not Track" is not mandatory for data collection firms nor would American Google users enjoy any EU protections.[46] So, while users can more easily monitor how others are using their information through tools like Me on the Web, they still cannot actively manage this information.

---

38. Dashboard has never allowed users control over their identity-linked information–Server logs, Cookies, and Interest-based advertising are the examples given by Google. Only the data associated with your google account is accessible on Dashboard–your search history when signed into your google account, or a shipping addressed you've stored in Google Checkout are the examples given by Google. *Is this everything?*, Google, http://support.google.com/accounts/bin/answer.py?hl=en&answer=162743.
39. *Id*.
40. Sam Grobart, *Google's New Data Sharing, and How to Deflect It*, N.Y. Times (Mar. 2, 2012), http://query.nytimes.com/gst/fullpage.html?res=940CE1DF1F30F931A35750C0A9649D8B63.
41. Sartain, *supra* note 30.
42. Silverman, *supra* note 30.
43. Sartain, *supra* note 30.
44. Tanzina Vega, *Risk and Riches in User Data: Opt-Out Provision Would Halt Some, but Not All, Web Tracking*, N.Y. Times (Feb. 26, 2012), http://www.nytimes.com/2012/02/27/technology/opt-out-provision-would-halt-some-but-not-all-web-tracking.html; Cecilia Kang, *Web Privacy Guidelines Viewed as Win for Google*, Wash. Post (Feb. 23, 2012), http://www.washingtonpost.com/business/economy/web-privacy-guidelines-viewed-as-win-for-google/2012/02/23/gIQAyyFhWR_story.html.
45. Claire Davenport, *EU Regulators Want Google to Halt New Privacy Policy*, Reuters (Feb. 3, 2012), http://www.reuters.com/article/2012/02/03/eu-google-idUSL5E8D31SC20120203 ("'The Commission therefore calls on Europe's data protection authorities to ensure that EU law is fully complied with in Google's new privacy policy.'" (quoting Viviane Reding, EU Justice Commissioner)).
46. Kang, *supra* note 44.

II. Lack of Current Legal Remedies for Managing Online Persona and Proposals for Future Legislation

There is a void of legal rights for Americans that might provide meaningful rights to manage one's personal information. Although the European Union has recently proposed a "right to be forgotten" as part of sweeping new regulation,[47] there are speech concerns that might make a similar proposal in the United States problematic. Perhaps a better alternative would be to give individuals an enforceable property right in their personal information to correct misinformation, a right that various European countries have, including the United Kingdom, Belgium, Germany, and Sweden.

A. Potential First Amendment Hurdles

There are various First Amendment hurdles to providing web users administrative rights to their online personas. It is extremely difficult to find legal support to correct even false information about one's self on the web. Courts have closed the door to many defamation[48] plaintiffs by expanding First Amendment protection over some false speech in order to avoid chilling effects on protected speech.[49] The Supreme Court reasoned that although there is no constitutionally protected value to false speech, some degree of false speech must be tolerated so as not to chill constitutionally-protected true

---

47. Press Release, European Commission, *Commission Proposes a Comprehensive Reform of Data Protection Rules to Increase Users' Control of Their Data and to Cut Costs for Businesses* (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=HTML&aged=0&language=EN&guiLanguage=en.

48. The common law doctrine most responsible for helping victims prevent or correct false information.

49. *See* Gertz v. Robert Welch, Inc., 418 U.S. 323, 340 (1974):

> Although the erroneous statement of fact is not worthy of constitutional protection, it is nevertheless inevitable in free debate. As James Madison pointed out in the Report on the Virginia Resolutions of 1798: "Some degree of abuse is inseparable from the proper use of every thing; and in no instance is this more true than in that of the press." 4 J. Elliot, Debates on the Federal Constitution of 1787, p. 571 (1876). And punishment of error runs the risk of inducing a cautious and restrictive exercise of the constitutionally guaranteed freedoms of speech and press. Our decisions recognize that a rule of strict liability that compels a publisher or broadcaster to guarantee the accuracy of his factual assertions may lead to intolerable self-censorship. Allowing the media to avoid liability only by proving the truth of all injurious statements does not accord adequate protection to First Amendment liberties. As the Court stated in New York Times Co. v. Sullivan, [376 U.S. 254, 270]: "Allowance of the defense of truth, with the burden of proving it on the defendant, does not mean that only false speech will be deterred." The First Amendment requires that we protect some falsehood in order to protect speech that matters.

speech.[50] Consequently, public figure plaintiffs must prove "actual malice,"[51] i.e. that the defendant knew of the falsity of the statement or recklessly disregarded the truth, to prevail in an action for defamation.[52] This stringent standard has proven nearly impossible to satisfy in a typical defamation suit.[53] "Public figures" include those who "by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention," have opened themselves up to more aggressive criticism.[54] Under a strict interpretation of this language, bloggers or other heavy users of social media could potentially be considered public figures, at least for limited purposes.[55]

Traditionally, courts have given the press considerable legal latitude, repeatedly holding that the press's right to report outweighed any the harm that it might cause.[56]

---

50. *Id*.; *cf*. Brian Leiter, *Cleaning Cyber-Cesspools: Google and Free Speech*, *in* THE OFFENSIVE INTERNET: PRIVACY, SPEECH, AND REPUTATION 150, 163 (Saul Levmore & Martha C. Nussbaum eds., 2011) ("Although it is common for cyber libertarians to talk as if *all* speech is immune to from legal regulation, even U.S. constitutional law permits the law to impose penalties for various kinds of 'low-value' speech, such as defamation.").

Professor Brian Leiter puts forth three rationales for permitting harmful speech: individual autonomy, democratic self governance, and the discovery of the truth ("the marketplace of ideas"). Leiter, *supra*. Professor Leiter explains the underlying principles behind these rationales by citing to John Stuart Mill:

> First, Mill thinks we are not justified in assuming that we are infallible: we may be wrong, and that is a reason to permit dissident opinions, which may well be true. Second, even to the extent our present beliefs are partially true we are more likely to appreciate the whole truth to the extent we are exposed to different beliefs that, themselves, may capture other parts of the truth. Third, and finally, even to the extent our present beliefs are *wholly* true, we are more likely to hold them *for the right kinds of reasons*, and thus more reliably, to the extent we must confront other opinions, even those that are false.

Id. at 164.

Professor Leiter challenges these rationales to the extent that they do not contribute to utility and are not even categorically interested in what is true and what is not. *Id*. ("For this line of argument to justify a type of speech, the speech in question must be related to the truth or our knowledge of it, and discovering this kind of truth must actually help us maximize utility.").

51. The phrase "actual malice" is a term of art. "Actual malice" does not mean ill will toward another or intent to interfere with the interests of another in an unprivileged manner. In fact, the Court has suggested that ill will or related mental states are an improper constitutional basis of imposing liability. *See* RESTATEMENT (SECOND) OF TORTS § 580A cmt. d (1977).

52. *Id*.

53. Mere negligence regarding the truth or falsity of a statement will not suffice; rather, actual subjective knowledge or reckless disregard of the statement's truthfulness is required. *See id*. § 600 cmt. b.

54. Gertz v. Robert Welch, Inc., 418 U.S. 323, 342 (1974).

55. *See* Yang-Ming Tham, Comment, *Honest to Blog: Balancing the Interests of Public Figures and Anonymous Bloggers in Defamation Lawsuits*, 17 VILL. SPORTS & ENT. L.J. 229, 247-48 (2010) (citing Anthony Ciolli, *Bloggers as Public Figures*, 16 B.U. PUB. INT. L.J. 255, 269-71 (2007)).

56. For the Civil Rights Movement, see *New York Times Co. v. Sullivan*, 376 U.S. 254 (1964). For Vietnam and the Pentagon Papers, see *New York Times Co. v. United States*, 403 U.S. 713 (1971). For Watergate, see *United States v. Nixon*, 418 U.S. 683 (1974).

Over time, they have consistently made the determination that it is better for some false information to be published than to suppress truthful information.[57] This reasoning relies in part on a presumption that there is an efficient marketplace of ideas in which truth prevails over falsehoods,[58] as well as the efficacy of rebutting false information with true information,[59] both of which have been questioned in recent

---

57. Although giving individuals property rights in their personal information might chill speech, there is some question as to whether this is First Amendment protected speech. Recently, the Second Circuit, in *Sorrell v. IMS Health Inc*., invalidated a Vermont Prescription Confidentiality law as a restriction on free speech. *Sorrell v. IMS Health Inc*., 630 F.3d 263 (2d Cir. 2010), *aff'd*, 131 S. Ct. 2653 (2011). In contrast, the First Circuit had upheld similar laws restricting access to government collected data by analyzing access to the information as commercial conduct and therefore outweighed by privacy interests. *IMS Health Inc. v. Ayotte,* 550 F.3d 42 (1st Cir. 2008); *IMS Health Inc. v. Mills*, 616 F.3d 7, 35 (1st Cir. 2010). Similarly, in a leading case on the collection and sale of government data, the U.S. Supreme Court upheld a Congressional Act that restricted State sales of driver personal information on the basis of consent. Reno v. Condon, 528 U.S. 141 (2000) (assessing the Congressional limits under the Commerce Clause to regulate States selling driver's personal information without consent).

58. The First Amendment concept of the "marketplace of ideas" is widely credited to Oliver Wendell Holmes, Jr. The instance most often associated with this attribution occurred in Holmes's dissent in *Abrams v. United States*, 250 U.S. 616, 630 (1919):

> Persecution for the expression of opinions seems to me perfectly logical. If you have no doubt of your premises or your power and want a certain result with all your heart you naturally express your wishes in law and sweep away all opposition...But when men have realized that time has upset many fighting faiths, they may come to believe even more than they believe the very foundations of their own conduct that the ultimate good desired is better reached by free trade in ideas...that the best test of truth is the power of the thought to get itself accepted in the competition of the market, and that truth is the only ground upon which their wishes safely can be carried out. That at any rate is the theory of our Constitution.

59. *Gertz*, 418 U.S. at 344:

> The first remedy of any victim of defamation is self-help—using available opportunities to contradict the lie or correct the error and thereby to minimize its adverse impact on reputation. Public officials and public figures usually enjoy significantly greater access to the channels of effective communication and hence have a more realistic opportunity to counteract false statements then private individuals normally enjoy.

The *Gertz* Court acknowledged in a footnote that "an opportunity for rebuttal seldom suffices to undo harm of defamatory falsehood," but still maintained its preference for rebuttal as the "first remedy." *Id*. at 344 & n.9 ("Indeed, the law of defamation is rooted in our experience that the truth rarely catches up with a lie.").

years.[60] Under this broad regime of First Amendment protection of false speech, defamation suits have slowed to a trickle.[61] As discussed, these First Amendment protections would likely prevent a general "right to be forgotten," such as the one proposed by the EU, and any other administrative rights to one's online persona would have to be narrowly tailored so as not to restrict or even chill First Amendment protected speech.

B. Other Legal Hurdles to Internet Enforcement

Many victims of harmful speech may find themselves without any legal remedy.[62] As discussed above, much of harmful speech is not actionable as a tort because it does not rise to the requisite level of harm.[63] Furthermore, Section 230 of the Communication Decency Act[64] absolves online service providers of most liability for speech related torts and

---

60. Scholars have argued that while the classicist's view of economic "free markets" has been repeatedly debunked over the past century, the classicist legal conception of a "marketplace of ideas" has remained unexamined. Joseph Blocher, *Institutions in the Marketplace of Ideas*, 57 Duke L.J. 821, 831-33 (2008). Furthermore, to the extent there is a functioning marketplace for information, its outcome is not necessarily "truth." *Id*. at 833 ("And even if people could reason perfectly, the market still might not function as Holmes envisioned, so long as their preferences are too unstable to permit the pursuit of a single "truth."). Research in the area has suggested that information consumers are not looking for the truth so much as information that confirms their own biases. *Id*. ("A related criticism suggests that even if the expression of ideas could be equalized, perhaps through government action, the efficiency of the marketplace of ideas would still be strictly limited by participants' imperfect ability to reason").

Similarly, there is some question as to the efficacy of rebuttal. Even when a rebuttal reaches the original recipient of the misinformation, evidence suggests that he will still believe the original misinformation over the correction. Lee Ross & Craig A. Anderson, *Shortcomings in the Attribution Process: On the Origins and Maintenance of Erroneous Social Assessments*, *in* Judgment Under Uncertainty: Heuristics and Biases 129, 149 (Daniel Kahneman, Paul Slovic & Amos Tversky eds., 1982) ("[B]eliefs can survive potent logical or empirical challenges. They can survive and even be bolstered by evidence that most uncommitted observers would agree logically demands some weakening of such beliefs. They can even survive the total destruction of their original evidential bases."). The name for this is "confirmation bias": a predisposition to believe information that supports a preconception, even when that information is later shown to be inaccurate. *Id*.

61. *See, e.g.*, Elena Kagan, *A Libel Story:* Sullivan *Then and Now*, 18 L. & Soc. Inquiry 197 (1993) (examining the history and impact of *New York Times Co. v. Sullivan*, and adverse consequences of the actual malice rule); John Koblin, *The End of Libel?*, N.Y. Observer (June 8, 2010), http://www.observer.com/2010/media/end-libel (following the trend of dwindling libel suits against mass media corporations).

62. Saul Levmore, *The Internet's Anonymity Problem*, *in* The Offensive Internet, *supra* note 50, at 50, 50 ("One can be the victim of soapbox invectives, crude thoughts recorded on a bathroom wall, malignant lines printed in a letter to the editor of a newspaper, hurtful statements or footage broadcast on television, or the same nasty words written in a comment on a blog site. The likelihood of injury seems greatest in the last of these settings, and it is there that the injured party is least protected by the law."); *see also* Leiter, *supra* note 50, at 164 ("Both tortious harms and dignitary harms are, in consequence, more harmful, than ever before.").

63. Leiter, *supra* note 50, at 164 ("Cyber cess-pools are thus an amalgamation of what I will call 'tortious harms' [harms giving rise to causes of action for torts such as defamation and infliction of emotional distress] and 'dignitary harms,' harms to individuals that are real enough to those affected and recognized by ordinary standards of decency, though not generally actionable.")

64. 47 U.S.C. § 230 (2006)

prohibits states from enacting any contrary legislation.[65] Section 230 (infamously) provides that "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[66] As a result, Section 230 protects most websites more broadly than traditional newspapers,[67] removing most, if not all, legal incentives that site owners might have to police their site.

C. European Union's Proposed "Right to Be Forgotten"

The closest attempt to granting web users administrative rights to their online personas has been a recent European Union proposal regarding privacy that drastically reforms their current regulations. The European's current rules regarding online privacy rules owe their origins to an international economic and trade forum in 1980 known as the Organization for Economic Cooperation and Development, which recommended seven basic principles for the protection and privacy of personal data.[68] These rights would eventually be integrated into a binding directive[69] requiring all members of the EU to implement protective procedures by 1998. The directive became known as the Data Protection Directive and placed heavy regulations on the use and acquisition of personal information.[70]

In January of 2012 the European Commission announced a proposal for reform provisions to the original directive.[71] The purpose of the reform was to bring the directive up to date with current Internet based data collection systems. EU leaders have described the new provisions as "a right to be forgotten."[72] Targeted largely at young people who are perhaps less discrete with what they post on the web,[73] the most powerful provision

---

65. "No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." § 230(e)(3).
66. § 230(c)(1).
67. Leiter, *supra* note 50, at 156 ("The effect of [Section 230] has been to treat cyber-cesspools wholly different from, for example, newspapers that decide to publish similar material. Whereas publishers of the latter are liable for the tortious letters or advertisements they publish, owners of cyber-cesspools are held legally unaccountable for even the most noxious material on their sites, even when put on notice as to its potentially tortious nature.")
68. The principals from the OECD are as follows: notice, purpose, consent, security, disclosure, access, accountability. For more information the OECD privacy principals, see *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Directorate for Sci., Tech. & Industry http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html.
69. A directive is binding on all member nations of the EU but the nation may choose the manner in which it meets the requirements listed in the directive.
70. Directive 95/46/EC, 1995 O.J. (L 281) 31.
71. Press Release, *supra* note 47.
72. *Id.*
73. *EU Proposes 'Right to Be Forgotten' by Internet Firms*, BBC (Jan. 23, 2012), http://www.bbc.co.uk/news/technology-16677370 ("These rules are particularly aimed at young people as they are not always as aware as they could be about the consequence of putting photos and other information on social network websites, or about the various privacy settings available." (quoting Viviane Reding, EU Justice Commisioner)).

added under this proposal allows individuals to remove any personal information from any database as long as there are no legitimate grounds to retain it.[74]

While it will take two years for the "Right to be Forgotten" to take effect from the date it is adopted, the current directive still keeps much of Europeans' private information secure. Google's newest privacy policy has been deemed by some EU officials to be in breach of the Directive.[75] The future of EU data privacy looks strong but many American companies that base their business models on easy procurement and distribution of user data see the protections as a hindrance to commerce and unenforceable because of complex jurisdictional issues.[76] Furthermore, many have criticized the proposed rules as being an unwarranted restriction on speech, with one critic analogizing it to George Orwell's *1984*, in which the "Ministry of Truth" uses a "memory hole" to prevent the spread of undesirable information.[77] The critic uses the example of former car racer and race administrator Max Moseley attempting to have a video of a Nazi-themed orgy removed.[78] Under U.S. law, Moseley would likely be considered a public figure and there would be First Amendment protections over speech regarding his involvement with that party, even if it turned out to be false.[79] For these reasons, the European solution may not be a workable one in the United States.

D. Legal Proposal for an American System: Property Rights to Personal Information

Perhaps a more workable solution is one that has been previously proposed – to grant individuals an enforceable but limited property right to their readily verifiable personal information, such as phone numbers or criminal history.[80] The property right could be structured in a way that its enforcement would have a limited chilling effect, with safe harbor provisions and limited monetary damages.[81]

An example of how a person might use the right to protect a more personal interest is illustrated in a *New York Times* op-ed, in which media lawyer and former social psychologist

---

74. *Id*.
75. Gabriele Steinhauser, *French Regulator Warns of Google Privacy Policy*, USA Today (Feb. 28, 2012, 12:18 PM), http://www.usatoday.com/money/industries/technology/story/2012-02-28/google-privacy-EU/53284914/1.
76. Kevin J. O'Brien, *E.U. to Tighten Web Privacy Law, Risking Trans-Atlantic Dispute*, N.Y. Times (Nov. 9, 2011), http://www.nytimes.com/2011/11/10/technology/eu-to-tighten-web-privacy-law-risking-trans-atlantic-dispute.html?pagewanted=all.
77. Jerry Britto, *What Europe's 'Right to Be Forgotten' Has in Common with SOPA*, Time Techland (Jan. 30, 2012), http://techland.time.com/2012/01/30/what-europes-right-to-be-forgotten-has-in-common-with-sopa/#ixzz1ovXIeS37.
78. *Id*.
79. *See supra* Part II.A regarding First Amendment restrictions on speech regulation.
80. Jamie Lund, *Property Rights to Information*, 10 Nw. J. Tech. & Intell. Prop. 1, 7–8 (2011), *available at* http://scholarlycommons.law.northwestern.edu/njtip/vol10/iss1/1.
81. *Id*.

Zick Rubin tells the story of how he was incorrectly listed in a Wikia.com article as having died in 1997.[82] Rubin humorously describes his predicament and his attempts to remedy it:

> I knew that the report of my death could be bad for business, so I logged into Wikia.com and removed the "1997." But when I checked a while later, I found the post had reverted to its prior form. I changed it again; again someone changed it back. Apparently the site had its doubts about some lawyer in Boston tinkering with the facts about American psychologists.
>
> When I complained to Wikia.com, I got a prompt and friendly reply from its co-founder, Angela Beesley, sending me her "kind regards" and telling me that she had corrected the article. But when I checked a week later, the "1944-1997" had returned. So I e-mailed her again (subject line: "inaccurate report that I am dead"), and got the following explanation:
>
> "My change to the page was reverted on the grounds that the info included in this article was sourced from Reber and Reber's the Dictionary of Psychology, third edition, 2001. Is it possible the page is talking about a different Zick Rubin? The article is about a social psychologist."
>
> I didn't doubt that the Dictionary of Psychology was a highly authoritative source, and yet I persisted in wondering why Reber—or, for that matter, Reber—would know more than I would about whether I was alive or dead.[83]

Rubin confirmed that the Reber and Reber book did list his death as being in 1997 and contemplated suing for defamation, but upon further inquiry discovered that "a false report of death is not on its own considered libelous."[84] Weeks later, Rubin checked the site again and noted, "Wikia.com had made the gutsy call that I was a reliable source on my own existence" and corrected the false report of his death.[85]

The property right could be structured to have minimal effect on speech by not providing for monetary damages and giving publishers a safe harbor.[86] Such a property right would not provide for general administrative rights over one's online persona, however it can be narrowly tailored enough to avoid the First Amendment's restrictions on regulation that chills protected speech.[87]

---

82. Zick Rubin, *How the Internet Tried to Kill Me*, N.Y TIMES, Mar. 13, 2011, at WK11.
83. *Id*.
84. *Id*.
85. *Id*.
86. Lund, *supra* note 80.
87. *Id*.

Conclusion

As Jeffrey Rosen warns, everyone has a digital and public dossier that can greatly impact their personal prospects. Companies like Google are allowing users to track their information without giving them any meaningful rights to control that information. Legal intervention would be necessary for web users to have "administrative rights" enabling them to manage the information available about them online. Although a general administrative rights such as the one proposed by the European Union would likely not be possible in the United States, an alternative may be a limited but enforceable property right to an individual's readily verifiable personal information that would allow individuals to ensure that their online persona is at least accurate. ■