Hastings Law Journal

Volume 64 | Issue 2 Article 6

12-2012

Note – The Right to Be Forgotten

Robert Kirk Walker

Note

The Right to Be Forgotten

ROBERT KIRK WALKER*

Information posted to the Internet is never truly forgotten. While permanently available data offers significant social benefits, it also carries substantial risks to a data subject if personal information is used out of context or in ways that are harmful to the subject's reputation. The potential for harm is especially dire when personal information is disclosed without a subject's consent. In response to these risks, European policymakers have proposed legislation recognizing a "right to be forgotten." This right would provide persons in European Union countries with a legal mechanism to compel the removal of their personal data from online databases.

However, only a limited form of the right to be forgotten—a right to delete data that a user has personally submitted—would be compatible with U.S. constitutional law. By itself, this limited right is insufficient to address the myriad privacy issues raised by networked technologies, but it is nevertheless an essential component of a properly balanced regulatory portfolio—as existing privacy tort law is inadequate in this context. As such, this Note argues that Congress should recognize this limited right through adoption of a default contract rule where an implied covenant to delete user-submitted data upon request is read into website terms of service contracts.

* J.D. Candidate at University of California, Hastings College of the Law, 2012. I would like to thank Professors Calvin R. Massey and Harry G. Prince for their feedback and guidance on this project.

Table of Contents

Introduction

Imagine: Allison Sprovveduto, a twenty-year-old college student, travels to Rome to participate in a year-long art history program. She is joined by a college classmate, Nell Silver, a young photographer who dreams of becoming a famous artist. In Rome, the women befriend a ragtag group of expatriate Americans and young European students who are more interested in contemporary Bacchanalia than in classical antiquity. Enterprising and ambitious, Nell uses her 35mm camera to document her new friends' socially transgressive and pharmacologically adventurous behavior, which she plans to compile into a book called *The Song of Sensual Freedom*, an homage to the work of her favorite photographer, Nan Goldin. Her friends love the idea and readily agree to model for her.

Halfway through the year, Allison meets a young Italian, Marco Canaglia, and they become romantically involved. In a libidinous fog, Allison and Marco voluntarily pose nude for Nell on several occasions, including once when they are photographed *in flagrante delicto*. Sadly, the relationship ends not long after the picture is taken, and the break-up is acrimonious.

When the school year ends, Allison and Nell return to the States, and Nell goes to New York, hoping to find a publisher for her work.

Though some editors are encouraging, none offers to publish her photographs. Undeterred, Nell decides to post her pictures online, hoping that *The Song of Sensual Freedom* will develop a substantial following on the Internet and jumpstart her career. Nell posts her pictures to the Web with imbedded metadata that identifies each subject by name and includes a descriptive caption (for example, "Allison Sprovveduto and Marco Canaglia making love, January 30"). However, Nell does not use any software to prevent users from downloading or otherwise copying the pictures.

Soon after Nell posts the pictures, Marco visits her website. Still angry about the break-up, he decides to get back at Allison for ending their relationship. He copies all the sexually explicit photos of Allison from Nell's site, and uploads them to myexgirlfriend.com, a pornographic website that specializes in "girlfriend revenge" photographs. Myexgirlfriend.com is part of a network of similar sites that trade pictures, and soon Allison's photos show up on adult websites all over the Internet—she is often identified by name.

A year later, Allison graduates from college and begins looking for a job in arts education. While putting together her resume, she decides to query her name in an online search engine. To her horror, the entire first page of results contains nothing but links to the sexually explicit photos taken in Italy. Some of the links point to Nell's website, but most point to "girlfriend revenge" websites, where users have annotated the photos with cruel comments about Allison's physical appearance and her imagined sexual proclivities.

It is not hard to foresee the potential fallout of this for Allison: lost job opportunities, strained personal relationships, reputational harm, damaged mental health, and so on. The above story is exaggerated for dramatic effect, but only slightly.[1] It is quite common for Internet users to reveal personal information they later regret,[2] or to have information posted about them that they wished had remained secret.[3] As numerous commentators have noted, information posted on the Internet is never truly forgotten.[4] On a basic technological level, once personal data[5] enter

1. *See, e.g.*, Kashmir Hill, *Revenge Porn with a Facebook Twist*, FORBES (July 6, 2011), http://www.forbes.com/sites/kashmirhill/2011/07/06/revenge-porn-with-a-facebook-twist (discussing defamation and involuntary nudity on the Internet).

2. *See, e.g.*, Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) (upholding denial of student's teacher certification due to picture on student's MySpace page captioned "drunken pirate").

3. *See, e.g.*, Balsley v. LFP, Inc., No. 1:08 CV 491, 2011 WL 1298180 (N.D. Ohio Mar. 31, 2011) (television anchor brought suit after photos and videos of her taken during "wet t-shirt" contest spread on the Internet).

4. *See, e.g.*, CHARLES J. SYKES, THE END OF PRIVACY 221 (1999) ("The struggle over privacy is the preeminent issue of the Information Age."); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT (2008); Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES MAG. (July

the online ecosystem, the original purpose behind disclosure becomes irrelevant. When allowed to flow freely—unrestrained by private commercial norms[6] or legal dictate—data are open to interpretation and use (or misuse) completely divorced from their original context.[7] Though society benefits from persistent data,[8] there are significant costs imposed as well—particularly when information disclosed for one specific purpose is ultimately used toward a completely different end.[9] The detrimental effects of permanently available data are most evident when personal information is disclosed without consent,[10] or when the damage caused by such disclosures is irreparable.[11] Data that cannot be deleted "will forever tether us to all our past actions, making it impossible, in practice, to escape them."[12]

What rights of control then, if any, should individuals have over personal information on the Internet? Should they be able to demand that information that is harmful to their reputations or that violates their privacy be permanently removed? If such rights exist, how do they interact with freedom of expression and the right of the press to gather news, as provided by the First Amendment?[13] How far do privacy rights

---

21, 2010), http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html.

5. In this Note, the term "personal data" is used to describe not only information that is used to identify a person (such as her birthdate, address, Social Security number, etc.) but also digital content that refers to a person, such a photographs or writings by or about her.

6. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 131 (1997) ("Individual responsibility, not regulation, is the principal and most effective form of privacy protection in most settings . . . . [T]he law should only provide limited, basic privacy rights . . . . The purpose of these rights is to facilitate—not interfere with—the development of private mechanisms and individual choice as a means of valuing and protecting privacy.").

7. *See generally* JAMES BOYLE, SHAMANS, SOFTWARE, AND SPLEENS: LAW AND THE CONSTRUCTION OF THE INFORMATION SOCIETY (1996); HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

8. *See, e.g.*, Kent Walker, *Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange*, STAN. TECH. L. REV., Dec. 2000, at 1, 7–21 (detailing the many benefits of abundant data).

9. *See, e.g.*, Snyder v. Millersville Univ., No. 07-1660, 2008 WL 5093140 (E.D. Pa. Dec. 3, 2008) (personal photo on MySpace resulting in denial of job certification).

10. *See, e.g.*, Hill, *supra* note 1.

11. For a pre-Internet example of the potential costs of unwanted public exposure, take Oliver Sipple, the man who thwarted an assassination attempt on President Gerald Ford on September 22, 1975. Unbeknownst to his family in the Midwest, Sipple was homosexual, and he wished for this fact to be kept secret by the press. Although Sipple entered the public eye only through an act of heroism, the California Court of Appeal held that there was a legitimate public interest in his private life. Sipple eventually committed suicide. *See* Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 669 (Cal. Ct. App. 1984) (holding that there was a legitimate public interest in Sipple's private life and that "he did not make a secret" of his sexual orientation, at least in San Francisco); *see also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 47–48 (2000).

12. VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 125 (2009).

13. *See infra* Subpart II.C.

extend temporally (do they ever expire and, if so, under what circumstances), spatially (in what jurisdictions may they be asserted), and personally (by and against whom may these rights be asserted)? Finally, are courts the proper venue for settling such disputes, or are other cultural, technological, or market-based approaches[14] preferable to adjudication?

In response to such questions,[15] European policymakers have called for the recognition of a "right to be forgotten," which would provide individuals with a legal mechanism to compel the permanent removal of their personal information from online databases.[16] The European Commission ("E.C.") has defined this right as, "the right of individuals to have their data . . . deleted when they are no longer needed for legitimate purposes."[17] While this right has yet to be statutorily adopted, European data privacy commissioners have indicated that some form of the right will likely be promulgated in the near future.[18]

This Note argues that only a limited form of the "right to be forgotten" is compatible with U.S. constitutional law. This form—a right to delete voluntarily submitted data—is substantially more limited in scope than the right to be forgotten proposed by the E.C. By itself, a right to delete voluntarily submitted data is insufficient to address the myriad privacy issues raised by networked technologies. It is, however, a necessary component of a properly balanced regulatory portfolio, as existing privacy tort law is inadequate and unconstitutional in this context.

Part I of this Note demonstrates how current U.S. privacy torts are both inadequate to deal with the legal issues that a right to be forgotten seeks to remedy and unconstitutional in light of First Amendment doctrine. Part II provides a brief historical overview of the theoretical differences between European and American privacy law, then outlines the substantive features of the right to be forgotten, as proposed by the

---

14. *See* CATE, *supra* note 6, at 131.

15. *See, e.g.*, Leigh Phillips, *EU to Force Social Network Sites to Enhance Privacy*, GUARDIAN (Mar. 16, 2011), http://www.guardian.co.uk/media/2011/mar/16/eu-social-network-sites-privacy (detailing European Union efforts to protect the "right to be forgotten").

16. *See* Press Release from Viviane Reding, Vice-President of the European Commission & E.U. Justice Commissioner, The EU Data Protection Reform 2012: Making Europe the Standard Setter for Modern Data Protection Rules in the Digital Age (Jan. 24, 2012) [hereinafter Reding, Making Europe the Standard Setter], *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26 .

17. Eur. Comm'n, *A Comprehensive Approach on Personal Data Protection in the European Union*, at 8, COM (2010) 609 final (Nov. 4, 2010) [hereinafter *E.U. Personal Data Protection*].

18. *See Daily Report: Europe Considers a Tough Online Privacy Law*, N.Y. TIMES (Jan. 24, 2012), http://bits.blogs.nytimes.com/2012/01/24/daily-report-europe-considers-a-tough-online-privacy-law; Graeme McMillan, *The Right to Be Forgotten: Europe Proposes New Online-Privacy Laws*, TIME (Jan. 25, 2012), http://techland.time.com/2012/01/25/europe-proposes-new-online-privacy-laws/?xid=gonewsedit.

E.C. Finally, Part III argues that the strongest basis for adopting a limited form of the right to be forgotten is as an implied contract term.

I. Current U.S. Legal Frameworks Provide Inadequate Data Privacy Controls

A. Defamation Law and the Right of Privacy

While popular accounts often characterize the legal and policy questions raised by Internet-based technology as unprecedented,[19] concerns about personal privacy and public reputation have long existed in legal debate.[20] Indeed, privacy and reputational rights are ancient in origin, dating back at least to Roman law.[21] In the Anglo-American common law tradition, civil and criminal penalties have long been imposed for making statements that are malicious, false, and disparaging to another person or group.[22] However, recovery for defamation is barred if the statements are true,[23] even if the statements are also extremely personal, embarrassing, or ruinous to another's reputation—regardless of the level of malice intended by the speaker.[24] As such, defamation law provides little shelter for a person's privacy: The secret and

---

19. *Cf.* Rosabeth Moss Kanter, *The Internet Changes Everything—Except Four Things*, Harvard Bus. Rev. Blog Network (May 26, 2011), http://blogs.hbr.org/kanter/2011/05/the-internet-changes-everythin.html.

20. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196–97 (1890).

21. For example, the Praetorian Edict, codified circa 130 A.D., provided a cause of action for shouting at a person in public contrary to good morals and for any act that might bring another person into ill-repute. *See* S.P. Scott, The Civil Law 315–17 (1932) (translating *Corpus Juris Civilis*, §§ 47.10.15.2, 47.10.15.25).

22. *See, e.g.*, Slanderous Reports Act, 1275, 30 Edw. 1, c. 34 (Eng.); *A Brief Narrative of the Case and Tryal of John Peter Zenger*, The Historical Society of the Courts of the State of New York (1734), *available at* http://www.courts.state.ny.us/history/elecbook/zenger_tryal/pg1.htm (establishing the precedent of truth as an absolute defense to defamation).

23. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279–80 (1964) (holding that a public official could win a suit for libel only if he or she could demonstrate "actual malice," meaning that the publisher had "knowledge that [the information] was false" or that the information was published with "reckless disregard of whether it was false or not"); *see also* Hustler Magazine v. Falwell, 485 U.S. 46, 56–57 (1988) (holding that the plaintiff could not recover for emotional distress caused by a parody advertisement because the statements made in the advertisement were so ridiculous that they were clearly not true); Gertz v. Robert Welch, Inc., 418 U.S. 323, 345–48 (1974) (holding that if negligence is present, a showing of actual malice is not necessary for defamation of a private person); Curtis Publ'g Co. v. Butts, 388 U.S. 130, 164 (1967) (extending the actual malice standard to include public figures, such as those people who "play an influential role in ordering society," in addition to public officials). *See generally Substantial Truth*, Citizen Media Law Project (July 22, 2008), http://www.citmedialaw.org/legal-guide/substantial-truth.

24. *See Hustler*, 485 U.S. at 55 ("'Outrageousness' in the area of political and social discourse has an inherent subjectiveness about it which would allow a jury to impose liability on the basis of the jurors' tastes or views, or perhaps on the basis of their dislike of a particular expression, and cannot, consistently with the First Amendment, form a basis for the award of damages . . . .").

uncomfortable facts of one's life are expressly unprotected by law. Therefore, an alternative basis is necessary for a successful tort action against a person making true but harmful statements.

In 1890, future Supreme Court Justice Louis Brandeis and Boston lawyer Samuel Warren addressed these issues in their classic law review article, *The Right to Privacy*.[25] Brandeis and Warren argued that a common law right to privacy exists that "secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[26] Brandeis's and Warren's article was written in response to privacy concerns raised by contemporaneous technological innovations, such as the Kodak Brownie camera (invented in 1884) and mass-circulation newspapers, which in 1890 had a readership of over eight million people.[27] Brandeis and Warren feared that the "sensationalistic press" would use these new technologies to upend social norms by "overstepping . . . the obvious bounds of propriety and of decency."[28] "Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[29] Their proposed remedy was to shield the "thoughts, sentiments, and emotions"[30] of private individuals from unauthorized public communication through a legal cause of action based on breach of confidence or breach of an implied contract.[31] For Brandeis particularly, stopping the invasion of private and domestic life was of utmost public concern; as he later commented, "the right to be let alone . . . [is] the right most valued by civilized men."[32] However, most applications in tort law of the principles Warren and Brandeis championed either have been excised from the body of U.S. law on constitutional grounds, or have atrophied to the point of feebleness.

B. Privacy Torts

By the middle of the twentieth century, four distinct torts had developed for violations of privacy: (1) intrusion on seclusion,

25. Warren & Brandeis, *supra* note 20, at 193.

26. *Id.* at 198.

27. *See* Daniel J. Solove et al., Privacy, Information, and Technology 9–11 (2006).

28. Warren & Brandeis, *supra* note 20, at 196.

29. *Id.* at 195.

30. *Id.* at 198.

31. *Id.* at 207.

32. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). *See* Warren & Brandeis, *supra* note 20, at 214–15 ("The design of the law must be to protect those persons with whose affairs the community has no legitimate concern, from being dragged into an undesirable and undesired publicity and to protect all persons, whatsoever; their position or station, from having matters which they may properly prefer to keep private, made public against their will.").

(2) misappropriation of name or likeness, (3) publicity placing a person in a false light, and (4) publicity given to private life.[33] The four torts protect distinct interests: Intrusion on seclusion protects mental well-being; misappropriation protects one's name and image; false light and publication of private facts protect one's reputation.[34]

Intrusion on seclusion prohibits the collection of information about an individual[35] and protects the areas of a person's life where they can reasonably expect to avoid intrusion.[36] An intrusion may be by physical means, such as breaking into a person's bedroom, or solely through the defendant's senses, such as peeping through a person's window.[37]

In contrast, misappropriation of name or likeness is not based on a physical invasion of private space, but on violation of the "interest of the individual in the exclusive use of his own identity."[38] This interest is "in the nature of a property right,"[39] and invasion usually occurs when a person's name or likeness is used to advertise a product, though the tort is not strictly limited to commercial exploitation.[40]

Disclosing facts about a person that present those facts to the public in a false light that would be "highly offensive to a reasonable person" is also potentially tortious.[41] The disclosed facts need not be defamatory[42]—true facts may also shine a false light—but the discloser must have acted with "actual malice" in order for the disclosure to be actionable.[43]

Finally, publicity given to private life (also referred to as public disclosure of a private fact) creates liability for publicizing true facts[44] of a highly personal nature that are not of legitimate concern to the public.[45]

---

33. *See* RESTATEMENT (SECOND) OF TORTS § 652B–E (1977); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

34. *See* RESTATEMENT (SECOND) OF TORTS § 652B–E; Prosser, *supra* note 33, at 398–423.

35. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. a.

36. *See* Pearson v. Dodd, 410 F.2d 701, 704 (D.C. Cir. 1969).

37. *See* RESTATEMENT (SECOND) OF TORTS § 652B cmt. b.

38. *Id.* § 652C cmt. a.

39. *Id.*

40. *Id.* § 652C cmt. b. *See, e.g.*, Gionfriddo v. Major League Baseball, 114 Cal. Rptr. 2d 307, 311 (Cal. Ct. App. 2001); Ainsworth v. Century Supply Co., 693 N.E.2d 510, 512 (Ill. App. Ct. 1998); *see also* 77 C.J.S. RIGHT OF PRIVACY AND PUBLICITY § 11 (West 2006).

41. RESTATEMENT (SECOND) OF TORTS § 652E.

42. *See, e.g.*, White v. Fraternal Order of Police, 909 F.2d 512, 523–24 (D.C. Cir. 1990); *see also* 77 C.J.S. RIGHT OF PRIVACY AND PUBLICITY § 13.

43. *See* RESTATEMENT (SECOND) OF TORTS § 652E. *See, e.g.*, Time, Inc. v. Hill, 385 U.S. 374, 390 (1967); Harris v. City of Seattle, 152 F. App'x 565, 567 (9th Cir. 2005); Peoples Bank & Trust Co. of Mountain Home v. Globe Int'l, Inc., 786 F. Supp. 791, 796 (D. Ark. 1992) ("[Plaintiff]'s experience could be likened to that of a person who had been dragged slowly through a pile of untreated sewage.").

44. *See, e.g.*, Leidholdt v. L.F.P. Inc., 860 F.2d 890, 895 (9th Cir. 1988).

45. *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 652D; Wagner v. City of Holyoke, 404 F.3d 504, 508 (1st Cir. 2005); *see also* Alfred Hill, *Defamation and Privacy Under the First Amendment*, 76 COLUM. L. REV. 1205, 1258–62 (1976) (positing that the "highly offensive to a reasonable person"

As the drafters of the Second Restatement of Torts (published in 1977) commented, the home life of an actress is of "legitimate and reasonable interest to the public," but the details of her sex life are not.[46] However, what is of legitimate interest to the public is highly subjective.[47]

While these so-called "Brandeis torts" protect different aspects of information privacy, common to all is the belief that there is a wall separating public and private life, and tort law is the mortar holding the wall together: "American privacy protections, at their metaphoric core, are the sorts of protections afforded by the walls of one's home. . . . [P]rotections become progressively weaker the further the affected person is from home."[48] The Brandeis torts presume that the public disclosure of certain categories of information would be, ipso facto, highly offensive to reasonable people, and that these categories can be judicially ascertained from prevailing social norms.[49]

Broad strokes sketched, let us return to the hypothetical to see which tort might offer a legal remedy for an embarrassed student who wishes to enjoin the publication of nude photographs on the Internet. In this case, intrusion on seclusion is inoperable, as the photographs were neither acquired through an unauthorized intrusion nor lacked the subjects' consent—Allison and Marco were willing participants at the time their photographs were taken. And, while Nell intended to use the photographs to benefit her artistic reputation, the subjects are private citizens, not public figures, and she did not accrue any benefit from their "reputation, prestige, social or commercial standing, public interest, or other values of . . . name or likeness."[50] Thus, misappropriation of likeness is also not actionable. While the photos arguably present their subjects in a bad light, the information contained in the photographs was true at the time it was acquired, and Nell did not act with malice, actual or otherwise, toward her subjects. So the only cause of action remaining is public disclosure of private facts that, as discussed in Part II, is most likely unconstitutional based on the First Amendment.

---

element of the tort is conceptually akin to unconscionability); Melville B. Nimmer, *The Right to Speak from* Times *to* Time*: First Amendment Theory Applied to Libel and Misapplied to Privacy*, 56 CALIF. L. REV. 935, 959 (1968) ("The gravamen in public disclosure [privacy] cases is degrading a person by laying his life open to public view.").

46. RESTATEMENT (SECOND) OF TORTS § 652D cmt. h.

47. *See* Jeffrey Rosen, *Free Speech, Privacy, and the Web That Never Forgets*, 9 J. ON TELECOMM. & HIGH TECH. L. 345, 349 (2011).

48. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1194 (2004).

49. Many scholars, however, find these presumptions dubious. *See, e.g.*, Rosen, *supra* note 47, at 348–49 ("[T]he Brandeis torts failed . . . because they all depend on some social consensus about what sort of invasions are highly offensive to a reasonable person or outrageous according to existing social norms.").

50. 77 C.J.S. RIGHT OF PRIVACY AND PUBLICITY § 11 (West 2006). *See, e.g.*, Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 86 (W. Va. 1984).

C. *FLORIDA STAR* AND THE "OBLITERATION" OF THE PUBLIC DISCLOSURE TORT

At first blush, the tort of public disclosure of a private fact seems viable as a remedy to unwanted dissemination of personal information, but American courts have consistently found that rights of freedom of speech, particularly those of the press, often trump privacy rights and preclude recovery.[51] When tort injury conflicts with free speech, the latter must win because, "in public debate [we] must tolerate insulting, and even outrageous, speech in order to provide adequate 'breathing space' to the freedoms protected by the First Amendment."[52]

The desiccation of the tort of public disclosure came under the heat of three Supreme Court cases: *Cox Broadcasting v. Cohn*,[53] *Smith v. Daily Mail Publishing*,[54] and *Florida Star v. B.J.F.*[55] In *Cox Broadcasting*, the Court considered whether the father of a deceased rape victim was entitled to damages from a broadcast television station that had identified the victim by name during coverage of her alleged rapist's trial.[56] The Court found for the station.[57] After reviewing the arguments put forward in *The Right to Privacy*, as well as the privacy torts contained in the Restatement,[58] the Court concluded that, "even the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears on the public record."[59] The Court, however, avoided the issue of whether a state could

---

51. *See* Harry Kalven, Jr., *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, LAW & CONTEMP. PROBS., Winter 1966, at 326, 335–38 (noting a substantial growth in the newsworthiness exception since *The Right of Privacy* was published); Rodney A. Smolla, *Privacy and the First Amendment Right to Gather News*, 67 GEO. WASH. L. REV. 1097, 1101 (1999) (arguing that the privacy tort has little relevance to law practice today); Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 293 (1983) ("[Privacy tort law] cannot coexist with constitutional protections for freedom of speech and press."). *See generally* David A. Anderson, *The Failure of American Privacy Law*, in PROTECTING PRIVACY 139 (Basil S. Markesinis ed., 1999). *But cf.* James Gordley, *When Is the Use of Foreign Law Possible? A Hard Case: The Protection of Privacy in Europe and the United States*, 67 LA. L. REV. 1073, 1099–100 (2007) (arguing that the reluctance of the Supreme Court to delineate public and non-public value in invasion of privacy cases led to overexpansion of free speech at the expense of legitimate privacy interests).

52. Snyder v. Phelps, 131 S. Ct. 1207, 1219 (2011) (quoting Boos v. Barry, 485 U.S. 312, 322 (1988)).

53. 420 U.S. 469, 493–96 (1975) (holding that the state cannot impose liability on a media outlet for publishing information found in a public record).

54. 443 U.S. 97, 105–06 (1979) (holding that there is no liability for publishing information lawfully acquired and in the public interest unless state interest is "of the highest order").

55. 491 U.S. 524, 541 (1989) ("[W]here 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 . . . .").

56. *Cox*, 420 U.S. at 472–74.

57. *Id.* at 491.

58. *See id.* at 487–97.

59. *Id.* at 494–95.

define certain private activities and information as off-limits from the press, and instead narrowed its holding to exempt from liability only the truthful publication of names obtained from public court records.[60] Two years later, in *Oklahoma Publishing Co. v. District Court ex rel. Oklahoma County*, the Court affirmed *Cox Broadcasting* and held that a newspaper company could not be held liable for publishing the events of a closed-door juvenile proceeding because the sitting judge allowed media into the courtroom.[61]

Then in *Daily Mail*, the Court suggested in dicta that all truthful publications made by the press are protected under the First Amendment, so long as the information was obtained from a lawful source.[62] After reviewing its holdings in *Cox Broadcasting*, the Court said that "if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order."[63] Finally, in *Florida Star*, the Court held 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*."[64] In dissent, Justice White argued that allowing a state to penalize the publication of truthful information only when "a state interest of the highest order" was involved effectively "obliterate[s] one of the most noteworthy legal inventions of the 20th century: the tort of the publication of private facts."[65]

Therefore, in light of the Court's view that the First Amendment guarantees the media a nearly unlimited right to publish truthful information, many scholars have questioned whether the tort of public disclosure is still valid:[66]

> [T]he tort's use is limited to cases in which the press publishes information that was unlawfully obtained and wholly unrelated to a matter of public significance. . . . Given the narrow class of information

60. *Id.* at 491.

61. *See* 430 U.S. 308, 311–12 (1977).

62. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979).

63. *Id.*

64. Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989) (emphasis added). The Court cabined this holding slightly: "We do 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 . . . ." *Id.*

65. *Id.* at 550 (White, J., dissenting).

66. *See* Franz Werro, *The Right to Inform v. the Right to Be Forgotten: A Transatlantic Clash*, GEORGETOWN UNIVERSITY CENTER FOR TRANSNATIONAL LEGAL STUDIES COLLOQUIUM, May 2009, at 285, 296, *available at* http://ssrn.com/abstract=1401357 ("After *Florida Star*, it appears there is little the states can do to prevent the media from disseminating sensitive information so long as that information is legally acquired . . . evinc[ing] a clear preference for broad First Amendment protections of the press over the privacy interests of individuals.").

> that fulfills the *Florida Star* requirements, the tort can no longer be an effective tool for protecting individual privacy.[67]

Thus, because of the public disclosure tort's tenuous constitutional status and the broad range of activities that qualify as protected speech,[68] there seems little merit to using the tort as a basis for enforcing online privacy rights.

D. Interlude: Privacy as Intellectual Property

There is a line of scholarly commentary arguing that private information should be treated as a form of intellectual property.[69] Proponents of this theory argue that individuals should be given the property rights to control their data,[70] and that personally identifiable information should be treated as "the property or quasi-property of the individual to whom it refers."[71]

In theory, intellectual property could provide a basis for a right to be forgotten, and one potential benefit of such a scheme would be that "a property approach would bind everyone, and not just those who are in contractual privity."[72] Another potential benefit is that, as a form of property, private information would be alienable, thus allowing for the creation of personal data markets where individuals could sell or barter their information.[73]

However, the privacy-as-property model is highly problematic from a constitutional standpoint. First, "[a] property right is, among other things, the right to exclude others; an intellectual property right in information is the right to exclude others from communicating information—a right to stop others from speaking."[74] As discussed in Subparts I.B and I.C, the Court has been consistently unwilling to allow

---

67. Jacqueline R. Rolfs, The Florida Star v. B.J.F.*: The Beginning of the End for the Tort of Public Disclosure*, 1990 Wis. L. Rev. 1107, 1127–28 (1990).

68. *See* Texas v. Johnson, 491 U.S. 397, 404 (1989) ("The First Amendment literally forbids the abridgment only of 'speech,' but we have long recognized that its protection does not end at the spoken or written word . . . . [W]e have acknowledged that conduct may be 'sufficiently imbued with elements of communication to fall within the scope of the First and Fourteenth Amendments.'").

69. *See, e.g.*, Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84. Geo. L. J. 2381, 2383–84 (1996) (describing personal information as property).

70. Lawrence Lessig, *The Architecture of Privacy: Remaking Privacy in Cyberspace*, Vand. J. Ent. L. & Prac., Spring 1999, at 56, 63 (suggesting that if the law gave individuals the rights to control their data, a new, beneficial market would follow).

71. Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373, 1420 (2000).

72. 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, 1063 (2000).

73. *See, e.g.*, Joshua Brustein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. Times, Feb. 13, 2012, at B3.

74. Volokh, *supra* note 72, at 1064–65.

speech restrictions on truthful publications in the absence of a state interest of the highest order.[75] So far, there have been no cases where state interests have been found to satisfy this standard. If the Court disallows recovery in speech-related, non-defamatory tort actions because of offense to the First Amendment, it is also highly unlikely that broadly applicable property rights that limit speech would pass constitutional scrutiny.[76]

Second, while quasi-IP rights of publicity afford some privacy protection, they are not generally applicable to private individuals. For example, to prevail on a misappropriation of likeness claim the plaintiff must show that the defendant, "appropriated for his or her own use or benefit the reputation, prestige, social or commercial standing, public interest, or other values of the person's name or likeness,"[77] a standard that is usually met only by celebrities and other well-known persons.

While a privacy-as-property theory does offer marked advantages over a privacy tort theory[78]—for example, it creates a legal entitlement that could be traded in a private data market—the underlying structure is not firmly rooted and is unlikely to survive judicial scrutiny on First Amendment grounds.[79] As discussed in Part III, only privacy guarantees grounded in contract law are capable of surviving First Amendment scrutiny and providing actionable remedies (albeit limited ones) to data privacy concerns.

II. ASSESSING THE RIGHT TO BE FORGOTTEN AS A REMEDY TO DATA PRIVACY LACUNAE

Current tort laws are insufficient to handle the personal privacy issues endemic to network-based technologies such as social networks, search engines, photo- and video-sharing sites, and the Internet generally.[80] To address these lacunae, privacy regulators in Europe have proposed the legislative recognition of a right to be forgotten that would allow individuals to demand permanent removal of their personal data

75. *See* Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989).

76. *Cf.* Marsh v. Alabama, 326 U.S. 501 (1946).

77. 77 C.J.S. RIGHT OF PRIVACY AND PUBLICITY § 11 (West 2006). *See, e.g.*, Crump v. Beckley Newspapers, Inc., 320 S.E.2d 70, 85–86 (W. Va. 1984).

78. *See generally* CATE, *supra* note 6, at 19–23 (summarizing various perspectives on privacy); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004)*; see also* Cohen, *supra* note 71 (expressing skepticism toward market solutions); Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1127–28 (2000) (advocating for market solutions to privacy issues, rather than new property rights); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609 (1999) (arguing for legislative enactment of "fair information practices" to address failures in the "privacy market").

79. *See* Volokh, *supra* note 72 (arguing that intellectual property rights in privacy are not easily defensible under free speech doctrine).

80. *See supra* Subpart I.B.

from websites. This Part will: (a) contrast the privacy traditions of Europe and the United States; (b) define the right to be forgotten as it is currently proposed by the E.C. and analyze the potential impact it would have on substantive free speech rights; and (c) discuss the First Amendment issues that the right to be forgotten would encounter if adopted in the United States.

A. European and U.S. Privacy Traditions

When Americans and Europeans speak of privacy, they are often talking about very different things. At the most basic level, the differences come down to conceiving of privacy as an aspect of personal liberty or as a component of personal dignity.[81] In the United States, where privacy is normally couched in the language of liberty, public policy is primarily concerned with protecting a citizen's "reasonable expectations of privacy" against impermissible government intrusion.[82] For example, American distrust of centralized power is embodied in the Fourth Amendment, which situates the home as the primary bulwark of privacy, and the government as its primary enemy.[83] In contrast, European privacy laws are primarily intended to safeguard an individual's dignity and public image, rather than to protect against governmental intrusions.[84] This attitude is reflected in Article 8 of the European Convention of Human Rights, which articulates "the right to respect for . . . private and family life."[85] Article 8 draws its inspiration from the French tradition of protecting citizens' reputations against compromising intrusions by others, particularly the media.[86] Because of this tradition, European courts tend to be less preoccupied with protecting free speech rights from government interference than American courts, and more willing to restrict speech if necessary to protect the dignitary[87] rights of citizens.[88] This judicial attitude is almost

81. *See* Whitman, *supra* note 48, at 1161.

82. *See* U.S. Const. amend. IV; Katz v. United States, 389 U.S. 347, 362 (1967) (Harlan, J., concurring).

83. *See* Whitman, *supra* note 48, at 1215.

84. *See, e.g.*, Rosen, *supra* note 11, at 5; Alan F. Westin, Privacy & Freedom (1967); Charles Fried, *Privacy*, 77 Yale L. J. 475, 477 (1968); Thomas Nagel, *Concealment and Exposure*, Phil. & Pub. Aff., Winter 1998, at 3.

85. Eur. Court of Human Rights, Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, ¶ 1, Nov. 4, 1950, 213 U.N.T.S. 221, 230. *See* Charter of Fundamental Rights of the European Union arts. 7–8, Dec. 7, 2000, 2000 O.J. (C 364) ("Respect for private and family life," and "Protection of personal data").

86. For example, French laws provides a "right to oblivion" (*le droit à l'oubli*), allowing a convicted criminal to object to the publication of the facts of her conviction once her sentence has been served. *See* Whitman, *supra* note 48, at 1171–80.

87. In this context, dignitary means "of or relating to one's interest in personal dignity," Black's Law Dictionary 522 (9th ed. 2009), rather than the more common usage of dignitary as "one who

diametrically opposed to the Supreme Court's view on the scope of free expression in *Florida Star*.[89]

This is not to say that Americans have no regard for their public reputation, or that Europeans are not concerned with the powers of the state, or even that the two concepts are necessarily mutually exclusive. Rather, privacy policy is best understood as existing on a spectrum between dignity and liberty, with European authorities drifting toward the former and American authorities toward the latter. Further, these default preferences are by no means determinative. For example, the privacy concerns that inspired *The Right of Privacy* are largely dignitary in nature—such as the potential of photographs to invade "the sacred precincts of private and domestic life," and the worry that "what is whispered in the closet shall be proclaimed from the house-tops."[90] Likewise, Europeans have long championed individual liberties that many Americans recoil from as grossly undignified, such as public nudity.[91] In the end, the policy differences here amount to more a question of *who* should be the protector of private information, not *what* information should be protected.[92] In Europe, the general trend has been for the state to intervene to protect citizens' privacy, whereas in the United States—in the interest of promoting personal liberty and free expression—individuals are left to protect their own privacy.

Thus, European rules that protect public reputation through government action[93] would meet significant hurdles in First Amendment doctrine if imported to the United States.[94] Nevertheless, there is a place

---

possesses exalted rank or holds a position of dignity or honor," *Dignitary Definition*, MERRIAM-WEBSTER.COM DICTIONARY, *available at* http://www.merriam-webster.com/dictionary/dignitary (last visited Oct. 2, 2012).

88. *See* Werro, *supra* note 66, at 289 ("[I]n the context of a conflict between [privacy rights] and the freedom of the press, the European Court [of Human Rights] . . . may well consider that in certain cases privacy rights trump the right to publish.").

89. *See* Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989) ("[W]here 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 . . . ."); *supra* Subpart II.C.

90. *See* Warren & Brandeis, *supra* note 20, at 195.

91. *See* Whitman, *supra* note 48, at 1200–01 ("Germans in particular appear fully nude in places like public parks (in the summer) and public coed saunas (in the winter) with a *sans-gêne* that Americans can hardly fathom . . . . The difference is not that Europeans refuse to be seen nude, but that they insist that they want to be the ones who should determine when and under what circumstances they will be seen nude. The difference is that the decision to appear nude, for Europeans, belongs to *their* control of *their* image.").

92. *See* Werro, *supra* note 66, at 299 ("Europeans trust in the government and distrust the market, while Americans take precisely the opposite view. . . . [P]rotecting 'privacy' in the vocabulary of both thus demands a shutting off of the flow of information to the institution that the respective society trusts the least."). For a comprehensive survey of the difference between privacy traditions in the United States and Europe, see Whitman, *supra* note 48.

93. *See, e.g.*, Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 294.

94. *See* Werro, *supra* note 66, at 286 ("The notion that constitutional rights could be balanced against each other and that the freedom to speak and inform could be balanced against a competing

for the right to be forgotten in American privacy law, as some operative features of the right can be separated out from the European legal and cultural context[95] and applied—without offense to the Constitution—through the mechanism of contracts.

B. Defining the Right to Be Forgotten: The European Commission Proposal

The right to be forgotten has its intellectual origin in French law, which provides a "right to oblivion" (*le droit à l'oubli*), wherein a convicted criminal may object to the publication of the facts of her conviction once she has served her sentence.[96] Ostensibly, the rationale for allowing a former convict to block the publication of facts about her crime is that once a person has been rehabilitated she should be free from having past criminality taint her reputation. Similarly, in the United States some states allow for sealing and expunging records of juvenile offenders on the presumption that youthful infractions should not follow a person into adulthood.[97]

Following this rationale, in 2010 the E.C. issued a communication proposing a comprehensive approach to personal data protection that would include a right to be forgotten extending to the personal data of all persons, not just rehabilitated criminals.[98] This right was defined as "the right of individuals to have their data . . . deleted when they are no longer needed for legitimate purposes."[99] This definition flows from European Union Privacy Directive Article 6, which provides that the laws of member-states must ensure personal information is "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."[100] Further, Article 12 of the Privacy Directive provides that each data subject has the right to "obtain from the controller . . . erasure or blocking of data,"[101] if the use of the data does not comply with Article 6.[102]

---

constitutional entitlement to the respect of one's private life does not seem to be an option under United States constitutional law.").

95. *See generally* Zittrain, *supra* note 4 (arguing for "reputation bankruptcy," which would allow people to wipe out certain categories of sensitive information periodically).

96. *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 Stan. L. Rev. Online 88, 88 (2012), *available at* http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten.

97. *See, e.g.*, Cal. Welf. & Inst. Code § 781 (West 2011). Information deletion mandates are not novel. For example, criminal records may be expunged, sealed, or destroyed, and DNA information taken from witnesses that is no longer necessary is deleted from databases in some states. *See* Mayer-Schönberger, *supra* note 12, at 158.

98. *E.U. Personal Data Protection*, *supra* note 17, at 8.

99. *Id.*

100. Council Directive 95/46, art. 6, 1995 O.J. (L 281) 31, 40 (EC).

101. *Id.* at art. 12.

102. This right of data protection is also included in Article 16 of the Treaty on the Functioning of

In early 2012, Vivian Reding, the European Commissioner for Justice, Fundamental Rights, and Citizenship, proposed that the European Parliament adopt the right to be forgotten[103] as a European Union-wide regulation.[104] She suggested that, if "an individual no longer wants his personal data to be processed or stored by a data controller, and if there is no legitimate reason for keeping it, the data should be removed from their system."[105] Under the proposed regulation, personal data is broadly defined as "any information relating to a data subject."[106] Upon request, website operators are required to "carry out the erasure without delay" unless the retention of data is "necessary" for exercising "the right of freedom of expression" as defined by the national laws of E.U. member-states.[107] The regulation also provides an exemption for "the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression."[108] Further, when deletion is requested, a website operator must take "all reasonable steps" to notify third parties with whom the data have been shared that deletion has been requested.[109] This duty is limited to what is technically feasible and does not require "a disproportionate effort."[110] Failure to comply with the regulation by any data controller could result in fines up to one million euros or two percent of the operator's annual worldwide income.[111]

Not surprisingly, heated scholarly debate followed the Commission's announcement. Most commentators focused on the proposal's potential chilling effects on free speech[112] and the economic

---

the European Union. *See* Consolidated Version of the Treaty on the Functioning of the European Union art. 16(1), Mar. 3, 2010, 2010 O.J. (C 83/47). S*ee generally* Jef Ausloos, *The 'Right to Be Forgotten'—Worth Remembering?*, 28 COMPUTER L. & SEC. REV 143 (2012).

103. *See* Reding, Making Europe the Standard Setter, *supra* note 16. For a thorough analysis of the proposed data protection legislation, see Christopher Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, PRIVACY & SEC. L. REP. (Feb. 6, 2012), and Somini Sengupta, *Europe Weighs Tough Law on Online Privacy*, N.Y. TIMES, Jan. 24, 2012, at B1.

104. In E.U. law, a directive requires member-states to adopt its requirements into national law, whereas a regulation applies throughout the European Union without need for ratification by the member-states. *See* Treaty of Rome art. 249, Mar. 25, 1957, *available at* http://eur-lex.europa.eu/en/treaties/dat/12002E/htm/C_2002325EN.003301.html ("[T]he European Parliament acting jointly with the Council, the Council and the Commission shall make regulations and issue directives, take decisions, make recommendations or deliver opinions.").

105. Reding, Making Europe the Standard Setter, *supra* note 16, at 5.

106. Eur. Comm'n, *Proposal for a Regulation of the European Parliament and of the Council*, at art. 4(2), COM (2012) 11 final (Jan. 25, 2012) [hereinafter *Commission Proposal*].

107. *Id.* art. 17(3).

108. *Id.* art. 80(1).

109. *Id.* art. 17(2).

110. *Id.* art. 13; *see also* Kuner, *supra* note 103.

111. *Commission Proposal*, *supra* note 106, at arts. 79(5)(c), (6)(c).

112. *See, e.g.*, Matt Warman, *EU 'Asking Google to Censor Web,'* TELEGRAPH (Feb. 14, 2012, 2:00 PM), http://www.telegraph.co.uk/technology/internet/9081619/EU-asking-Google-to-censor-web.html;

impact of compliance.[113] It remains to be seen what parts of the proposal, if any, the European Parliament will enact[114] and whether the promulgated regulations will be enforced as written.[115] If it were enacted without alteration, the proposal represents the strongest version of the right to be forgotten currently under consideration by European policymakers.

Based on the Commission Proposal, a working definition of the right to be forgotten has two parts: (1) An individual has the right to have her personal data deleted from a website if doing so does not infringe free expression (which explicitly includes journalism and artistic and literary expressions); and (2) website operators must remove such data from their servers without delay, in addition to making best efforts to remove it from any third-party servers with which the data has been shared.

C. Does the Right to Be Forgotten Violate the First Amendment?

"The American resistance to [privacy rights] has always been a resistance founded on two values in particular: the value of the free press, and the value of the free market."[116] This has been particularly true when privacy rights interfere with newsgathering. In the United States, the media is expected to "uncover the truth and report it—not merely the truth about government and public affairs, but the truth about people."[117] The law protects these expectations, and "when they collide with expectations of privacy, privacy almost always loses."[118] Thus, some scholars have predicted that if the right to be forgotten were adopted in the United States, it would fare no better under constitutional scrutiny than the Brandeis torts have.[119]

Jane Yakowitz, *More Bad Ideas from the E.U.*, Forbes (Jan. 25, 2012, 3:57PM), http://www.forbes.com/sites/kashmirhill/2012/01/25/more-bad-ideas-from-the-e-u.

113. *See, e.g.*, *Privacy Laws: Private Data, Public Rules*, Economist, Jan. 28, 2012, at 47.

114. *See* Kuner, *supra* note 103 ("Completion of the EU legislative process is a politically charged undertaking that will likely take at least one to two years to complete, and will require approval by the Council of the European Union and the European Parliament; the Proposed Regulation is to take effect two years after that. This lengthy process also makes it practically certain that there will be changes (potentially major ones) to the Proposal.").

115. *See* Rosen, *supra* note 96, at 92 ("Europeans have a long tradition of declaring abstract privacy rights in theory that they fail to enforce in practice."); *see also* Kuner, *supra* note 103 ("Article 17 will likely prove difficult to apply in practice, and may have a chilling effect on use of the internet in the EU.").

116. Whitman, *supra* note 48, at 1208.

117. *Id.* at 1197.

118. *Id.*; *See* Fla. Star v. B.J.F., 491 U.S. 524, 540–41 (1989).

119. *See* Werro, *supra* note 66, at 298 ("[T]here is no reason to think that a right to be forgotten stands any chance of developing under the current *Cox* and *Florida Star* regime in American privacy law.").

This may not be the case. Consider the three primary groups of actors who are implicated by the right to be forgotten: data subjects, content creators, and third-party websites like search engines and aggregators.[120] The first group covers people who are the subjects of data posted, stored, or collected online. The second group contains persons who post data online that qualifies as protected speech, such as blog posts, pictures on Facebook, videos on YouTube, product comments in online stores, et cetera. The third category comprises websites that display or link to material created by others (for example, news feeds, search engines, audiovisual databases).[121] In the interaction between these three groups, the salient question is whether granting data subjects the right to compel the removal of personal information from the Internet would infringe upon the First Amendment rights of either content creators or third-party websites.[122] Or, in terms of the hypothetical: (1) Would granting Allison, a data subject, the right to require that Nell, a creator, remove the offending pictures from her website violate Nell's free speech rights; and (2) would granting this right allow Allison to compel that the pictures be removed from third-party websites, such as myexgirlfriend.com?

Turning to the first question, photography is a form of expressive conduct that is protected by the First Amendment.[123] Accordingly, Nell

---

120. The term "content aggregator" is being used here to denote passive compilers of data who use automated processes (for example, search engine algorithms) rather than manual selection to populate their databases. While many sites both aggregate and create data, those that actively create, edit, or publish original content would fall in the creator category in this taxonomy, rather than in the content aggregator category. Therefore, journalistic websites such as online newspapers, magazines, blogs, et cetera are creators, even if their First Amendment rights differ from those enjoyed by private individuals. While these differences are not insignificant from the standpoint of First Amendment doctrine, they do not affect our analysis here. *See* Chris Conley, *The Right to Delete*, ACLU OF NORTHERN CALIFORNIA 53, 56 (last modified Mar. 23, 2010), *available at* http://www.aaai.org/ocs/index.php/SSS/SSS10/paper/view/1158 ("[A] right to delete may have additional impact on freedom of the press, in the sense that a right to delete incriminating records from one's past reduces or eliminates the press's ability to (re)publish these incidents if they return to relevance.").

121. This taxonomy is derived, in part, from questions posed by Peter Fleischer, Global Privacy Counsel for Google. *See* Peter Fleischer, *Foggy Thinking About the Right to Oblivion*, PRIVACY . . . ? (Mar. 9, 2011), http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html (arguing that a "right to be forgotten" is a concealed form of censorship).

122. *See* Conley, *supra* note 120, at 54–57.

123. *See* Texas v. Johnson, 491 U.S. 397, 404 (1989) ("The First Amendment literally forbids the abridgment only of 'speech,' but we have long recognized that its protection does not end at the spoken or written word. . . . [W]e have acknowledged that conduct may be 'sufficiently imbued with elements of communication to fall within the scope of the First and Fourteenth Amendments.'"). Similarly, the fact that photographs are sexually explicit does not preclude them protection under the First Amendment. *See* Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 126 (1989) ("Sexual expression which is indecent but not obscene is protected by First Amendment . . . ."); Miller v. California, 413 U.S. 15, 39 (1973) ("Today we would add a new three-pronged test [for obscenity]: (a) whether the average person, applying contemporary community standards would find the work, taken as a whole, appeals to the prurient interest, . . . (b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and (c) whether

has a constitutional right to make photographs and to display her work in public fora such as her website. However, sexually explicit pictures also convey information related to the people photographed, and so the pictures fall within the scope of data that are subject to the Commission Proposal's right to be forgotten: "any information relating to a data subject."[124] So, Nell's free speech rights stand in direct opposition to Allison's putative right to be forgotten. However, as discussed in Subpart II.B, the Commission Proposal also provides that data may not be deleted when it is necessary for exercising "the right of freedom of expression," as defined by national laws.[125] Under *Daily Mail* and *Florida Star*, truthful publications of lawfully obtained information[126] may be constrained only when the restriction is "narrowly tailored to a state interest of the highest order."[127]

While truthful publications are not automatically afforded First Amendment protection,[128] there have been no cases where the Court has found an individual's privacy rights are themselves a "state interest of highest order." Furthermore, given that the *Florida Star* Court held that a newspaper could not be constrained from publishing the full name of a sexual assault victim,[129] it is all but inconceivable that a court would find that the privacy rights of a willful sexual actor who subsequently regretted her decisions are of sufficient state interest to justify a restraint on speech: "[A]bsent exceptional circumstances, reputational interests alone cannot justify the proscription of truthful speech."[130] Therefore, Allison would not have grounds to compel the removal of the photographs from Nell's website based on the right to be forgotten, as doing so would violate Nell's First Amendment rights.[131] Thus, by

---

the work, taken as a whole, lacks serious literary, artistic, political, or scientific value." (alteration in original) (internal quotation marks omitted)).

124. *See Commission Proposal*, *supra* note 106, art. 4(2).

125. *Id.* art. 17(3)(a).

126. It remains an open question whether liability would arise from the publication of truthful information that was obtained by illegal means. *See* Bartnicki v. Vopper, 532 U.S. 514, 528, 534 (2001). The First Amendment interest in publishing matters of public importance outweighs privacy rights if the media outlet plays no part in illegal interception. *Id.* at 534. "However, [the Pentagon Papers case] raised, but did not resolve, the question 'whether, in cases where information has been acquired *unlawfully* by a newspaper or by a source, government may ever punish not only the unlawful acquisition, but the ensuing publication as well.'" *Id.* at 528 (quoting Fla. Star v. B.J.F. 491 U.S. 524, 535, n.8 (1989)).

127. Fla. Star v. B.J.F., 491 U.S. 524, 541 (1989). *See* Smith v. Daily Mail Publ'g, 443 U.S. 97, 103 (1979).

128. *See Fla. Star*, 491 U.S. at 541 ("We do 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 . . . .").

129. *Id.* at 537–41.

130. Butterworth v. Smith, 494 U.S. 624, 634 (1990).

131. *See supra* Subpart II.C.

extension, it seems that the right to be forgotten could only be applied by a data subject against a content creator under "exceptional circumstances" of the "highest order" of state interest. Personal privacy and reputational harm are not such interests.

Similarly, the First Amendment would preclude Allison from compelling the removal of the photographs from third party websites, including myexgirlfriend.com. Even though Marco acquired the photographs through illicit means (that is, by copying Nell's copyrighted images without authorization), Nell lawfully created the original photographs. Unlike Nell, Allison does not have any proprietary interests in the photographs,[132] and she cannot compel Nell to enforce her copyrights against third-party infringers. Likewise, if there is no basis for a data subject to assert the right to be forgotten against a content creator,[133] then there is also no basis for a claim against third parties who copy, link to, or otherwise republish the offending data.[134] Given the breadth of First Amendment protections following *Florida Star*, the speech rights of creators and third-party websites trump the privacy rights of data subjects. Thus, without Nell's assistance, Allison has no constitutionally valid means to compel websites displaying the photographs to remove them.

However, even though applying the full weight of the right to be forgotten would be unconstitutional, the First Amendment does not proscribe all potential data deletion rights. The First Amendment not only grants Internet users a right to speak, but also the right *not* to speak. "The right to speak and the right to refrain from speaking are complementary components of the broader concept of 'individual freedom of mind.'"[135] Moreover, the First Amendment does not compel anyone to speak,[136] nor does it forbid voluntary agreements not to speak.[137] Therefore, just as Nell may exercise her right to free expression

---

132. The situation might be different if Allison was a well-known person, in which case a state right-of-publicity tort might be applicable.

133. *See Fla. Star*, 491 U.S. at 541.

134. *See id.*

135. Wooley v. Maynard, 430 U.S. 705, 714 (1977) (quoting W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 637 (1943)). *See* Robert A. Sedler, *The First Amendment Right of Silence* (Wayne State Univ. Law School Research Paper Series, No. 07-39, 2007), *available at* http://ssrn.com/abstract=1031505.

136. *See* Pac. Gas & Elec. Co. v. Pub. Utils. Comm'n, 475 U.S. 1, 11 (1986) ("[The First Amendment contains a] freedom *not* to speak publicly, one which serves the same ultimate end as freedom of speech in its affirmative aspect."); W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 645 (1943) (Murphy, J., concurring) ("The right of freedom of thought and of religion as guaranteed by the Constitution against State action includes both the right to speak freely and the right to refrain from speaking at all . . . ."); *see also* Anna M. Taruschio, *The First Amendment, the Right Not to Speak and the Problem of Government Access Statutes*, 27 FORDHAM URB. L.J. 1001, 1012–19 (1999).

137. *See* Cohen v. Cowles Media, 501 U.S. 663, 672 (1991) (holding that contracts not to speak are enforceable without First Amendment problems); *cf.* Branzburg v. Hayes, 408 U.S. 665, 681 (1972) (First Amendment case law does not command the press to publish what it would rather withhold).

by posting photographs on her website, she also has a right to stop speaking by removing the pictures, thereby muting the instrument of her speech. Similarly, nothing in the First Amendment forbids Nell from entering into a contract with her website hosting company where she could mandate that data she posts be permanently removed from their servers upon request. In instances where a user submits her own personal data to a website and then demands removal, both actions are variations on the same underlying constitutional right. As such, a circumscribed version of the right to be forgotten—a right to delete voluntarily submitted data—would not offend the First Amendment.

III. The Contractual Basis for a Right to Delete Voluntarily Submitted Data

Establishing a statutory right to delete voluntarily submitted data would help fulfill user's expectations of data privacy, align international privacy norms, and drive the market for improved data management technologies. Furthermore, such a right could be legislatively enacted as a default contract rule without running afoul of the U.S. Constitution.[138]

The main advantage of contracting for privacy is that the contract model does not endorse any right to stop others from speaking that would offend the First Amendment. Rather, it endorses a right to stop people from breaking their promises.[139] In *Cohen v. Cowles Media*, the Supreme Court held that contracts not to speak—that is, promises made not to reveal information or say certain things—are enforceable and do not violate the First Amendment.[140] Similarly, when persons have an expectation that their private data will be kept secret, then courts may infer an implied contract[141] of confidentiality or apply the doctrine of promissory estoppel to enforce this expectation of privacy.[142] "In many

138. *See* Volokh, *supra* note 72, at 1051 ("While privacy protection secured by contract is constitutionally sound, broader information privacy rules are not easily defensible under existing free speech law."). *But cf.* Jessica Litman, *Information Privacy/Information Property*, 52 Stan. L. Rev. 1283, 1308–12 (2000) (arguing for tort action against unauthorized disclosure of personal data based on "breach of trust").

139. Volokh, *supra* note 72, at 1061.

140. *See Cowles Media*, 501 U.S. at 670–72. This holding also applies to promises that are enforceable under the equitable doctrine of promissory estoppel and to implied contracts.

141. Implied terms in contracts come in two flavors. First, implied terms may be derived from judicial precedent or statute (for example, under the Uniform Commercial Code § 2-306(1), a term of best efforts is implied in exclusive dealings contracts). Such terms are referred to as implied-in-law. Terms that are inferred based on the circumstances surrounding the formation of the contract, such as prior transactions between the parties, industry custom, specific definition of other contractual terms, etc., are referred to as implied-in-fact. For our purposes, a right to delete voluntarily submitted data could be read into a contract in either form without altering the substantive right granted.

142. *See* Restatement (Second) of Contracts § 4 cmt. a (1979); Volokh, *supra* note 72, at 1058–59; Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global*

contexts, people reasonably expect—because of custom, course of dealing with the other party, or all the other factors that are relevant to finding an implied contract—that part of what their contracting partner is promising is confidentiality."[143] As such, the enforcement of privacy contracts does not offend free speech rights, as the government is not restricting speech, but rather enforcing obligations that the would-be speaker has voluntarily assumed.[144]

Privacy contracts also avoid the need for courts to determine whether disclosures are "highly offensive to a reasonable person,"[145] as required by the Brandeis torts.[146] Rather, privacy contracts rely on a more objective, purpose-limitation principle whereby "the recipient of personal information can only use that information for the purposes to which [the discloser] consented, and no[t] others."[147] Courts regularly look to usage in trade, course of dealings, standard business practices within an industry, et cetera to interpret implied-in-fact terms in commercial contracts. If Congress enacted legislation requiring implied privacy terms in website terms of service contracts, these same interpretative and evidentiary principles could be used to assess a person's expectations of data privacy at the time of initial disclosure.

Framing privacy rights in contractual terms also has the benefit of increasing data privacy protections across the Internet by standardizing website terms of service agreements and privacy policies. Currently, website privacy policies vary dramatically, even within a network of sites operated by a single company.[148] Policies are also subject to change—

Information Economy, 87 CALIF. L. REV. 751, 768 (1999) (book review) ("[P]olls show that many people who disclose to others information about themselves for a particular purpose (e.g., to get credit or to be treated for a disease) believe that their disclosures have been made under an implied, if not an explicit, pledge to use the data only for that purpose.").

143. Volokh, *supra* note 72, at 1057–58 (footnote omitted).

144. *See, e.g.*, Samuelson, *supra* note 78, at 1155–57 (arguing that nonconsensual communication of personal data by merchants should be actionable under a quasi-trade-secret theory, supported by *Cohen v. Cowles Media*); s*ee also Cowles Media*, 501 U.S. at 671. *See generally* Scott Shorr, Note, *Personal Information Contracts: How to Protect Privacy Without Violating the First Amendment*, 80 CORNELL L. REV. 1756 (1995).

145. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977); *supra* Subpart I.B.

146. *See, e.g.*, Rosen, *supra* note 47, at 348–49 ("[T]he Brandeis torts failed . . . because they all depend on some social consensus about what sort of invasions are highly offensive to a reasonable person or outrageous according to existing social norms.").

147. MAYER-SCHÖNBERGER, *supra* note 12, at 136. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 174–76 (2007) (arguing for an expansion of breach of confidence laws to include embarrassing posts by others in violation of one's privacy settings); Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 130–32 (2007).

148. For example, prior to consolidation into one single privacy policy on March 1, 2012, Google had sixty separate privacy policies for its various websites and services, each with its own set of terms and conditions, some of which were mutually exclusive and contradictory. *See Policies & Principles*, GOOGLE, *available at* https://www.google.com/intl/en/policies (last visited Oct. 2, 2012); *see also* Claire Cain Miller, *Google to Update Privacy Policy to Cover Wider Data Use*, N.Y. TIMES BITS BLOG (Jan.

often suddenly—at the sole discretion of website operators.[149] Further, the software architecture of many websites incorporates data-gathering technologies provided by third parties, such as advertising networks,[150] that collect information about users either on behalf of the host website or for their own business purposes. For example, according to a *Wall Street Journal* investigative report, "the nation's 50 top websites on average installed 64 pieces of tracking technology onto the computers of visitors, usually with no warning."[151] Certain types of data collection are subject to statutory restriction, such as financial data,[152] healthcare information,[153] and information collected about children.[154] But most personal data collected and stored by website operators (for example, a user's geographic location, web search and browsing history, personal messages and information shared on social media sites, and files stored "in the cloud") are not currently subject to regulation.[155]

Additionally, personal data collection and retention practices are also largely out of sync with public perception of what data privacy rights should exist.[156] For example, a 2009 survey by the Universities of Pennsylvania and California found that more than 80% of Americans believe websites should not track their behavior for advertising, and that more than 90% believe advertisers should be required by law to stop tracking on request.[157] A follow-up study in 2010 found that 88% of young adults surveyed[158] said that the law should require websites to

---

24, 2012, 4:30 PM), http://bits.blogs.nytimes.com/2012/01/24/google-to-update-its-privacy-policies-and-terms-of-service.

149. *See, e.g.*, Caroline McCarthy, *Do Facebook's New Privacy Settings Let It off the Hook?*, CNET NEWS (May 26, 2010, 12:07 PM), http://news.cnet.com/8301-13577_3-20006054-36.html; Jon Swartz, *Facebook Draws Protests on Privacy Issue*, USA TODAY (May 13, 2010, 9:31 PM), http://www.usatoday.com/money/media/2010-05-14-facebook14_ST_N.htm; Jessica E. Vascellaro, *Facebook Grapples with Privacy Issues*, WALL ST. J. (May 19, 2010), http://online.wsj.com/article/SB10001424052748704912004575252723109845974.html.

150. *See Advertising Network*, WIKIPEDIA, http://en.wikipedia.org/wiki/Advertising_network (last visited Oct. 2, 2012).

151. Julia Angwin, *The Web's New Gold Mine: Your Secrets*, WALL ST. J. (July 30, 2010, 5:59 PM), http://online.wsj.com/article/SB10001424052748703940904575395073512989404.html.

152. *See* Gramm-Leach-Bliley Act, 12 U.S.C. §§ 24, 78, 248, 377, 1831, 1848, 2908 (2006); 15 U.S.C. § 80 (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006).

153. *See* Health Insurance Portability and Accountability Act, 29 U.S.C. § 1181 (2006), 42 U.S.C. §§ 1320, 1395 (2006).

154. *See* Children's Online Privacy Protection Act, 15 U.S.C. § 6501 (2006).

155. Some scholars have argued that this lack of regulation is preferable from both a market and public policy perspective. *See* CATE, *supra* note 6, at 131.

156. *See, e.g.*, Lothar Determann, *Data Privacy in the Cloud: A Dozen Myths and Facts*, COMPUTER & INTERNET LAWYER, Nov. 2011, at 1, 2–3.

157. JOSEPH TUROW ET AL., CONTRARY TO WHAT MARKETERS SAY, AMERICANS REJECT TAILORED ADVERTISING 14, 23, *available at* http://ssrn.com/abstract=1478214.

158. Those surveyed were aged 18 to 24.

delete all stored information about users,[159] and 62% said there should be a law giving people the right to know all the information that a website has collected about them.[160] The authors of these surveys found that, "large percentages of young adults are in harmony with older Americans when it comes to sensitivity about online privacy."[161] These empirical results indicate a broad cultural preference for having the ability to opt-out of data collection and to have personal data removed on demand.

The existence of cultural preferences concerning online privacy does not necessarily imply that a user would expect these preferences to be reflected in a website terms of service agreement: Users may wish one thing, but expect or even accept its opposite. However, just because users might not currently expect contractual data privacy, this does not present a barrier against a legislature requiring that an implied data deletion term be included in all website terms of service contracts. Indeed, such legislative action is likely necessary for data retention practices to ever come into line with popular preferences, as website operators have relatively weak incentives to do so on their own. For example, data storage is increasingly inexpensive,[162] and website operators benefit financially from retaining data for future use—such as selling their databases to other companies or "mining" them for the purposes of targeted advertising or marketing.[163] Moreover, website operators are often slow to enforce their own privacy procedures.[164] While websites that publicly violate user privacy norms risk reputational damage and loss of goodwill to their corporate brands, so long as all operators maintain similarly weak data privacy and protection standards, the headline sensitivity for any individual company is minimized.[165] Thus establishing an explicit legal basis for users to demand the deletion of data, accompanied by strong penalties for non-compliance, would act as

159. *See* CHRIS HOOFNAGLE ET AL., HOW DIFFERENT ARE YOUNG ADULTS FROM OLDER ADULTS WHEN IT COMES TO INFORMATION PRIVACY ATTITUDES AND POLICIES? 11 tbl.5 (2010), *available at* http://ssrn.com/abstract=1589864.

160. *Id.* at 11 tbl.4; *see also* Danah Boyd & Alice Marwick, *Social Privacy in Networked Publics: Teen's Attitudes, Practices, and Strategies* (June 2, 2011) (Privacy Law Scholar's Conference working paper).

161. HOOFNAGLE, *supra* note 159, at 3.

162. *See* FTC, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 46–47 (2010) [hereinafter FTC STAFF REPORT].

163. *See* Angwin, *supra* 151; *see also* FTC STAFF REPORT, *supra* note 162, at 36–52.

164. *See, e.g.*, Nick Clayton, *'Deleted' Facebook Photos Still Online After Three Years*, WALL ST. J. (Feb. 7, 2012, 7:13 AM), http://blogs.wsj.com/tech-europe/2012/02/07/deleted-facebook-photos-still-online-after-three-years.

165. This, in many respects, is an example of the economic public goods problem, where society as a whole would benefit from the creation of a good or service (for example, a lighthouse), but no individual actor has incentive to create this good because of the disproportionate burden of doing so relative to the individual benefit.

a market lever to pressure website operators into adopting deletion protocols that better align with users' professed preferences.[166]

The contract approach to data privacy, however, is not without significant limitations. First, and most restrictive, are the requirements of contractual privity. While "many jurisdictions around the world conceptualize information privacy rights as binding all subsequent users of an individual's personal information,"[167] 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.[168] Other parties do not. Thus, 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.[169] As such, contracts can only protect personal data that are voluntarily submitted by a user to a website with whom she has a contract (explicit or implied), and a third party cannot compel the deletion of embarrassing data submitted by another person.

Applying this to our hypothetical, Allison would not have standing to force myexgirlfriend.com to remove the photos of her based on breach of contract, and likewise neither would Nell.[170] Only Marco, the villain of our story, is in contractual privity with myexgirlfriend.com, and only he could compel deletion of the photographs. Thus, a right to delete voluntarily submitted data does not provide a surrogate cause of action for the public disclosure tort and is quite limited in the relief it could provide to victims of public humiliation.

That said, a large portion of data uploaded to websites is done by users in privity with the website. For example, users that post comments on their Facebook walls, submit videos to YouTube, or send out messages on Twitter would all be in privity with these respective websites. In such cases, if the terms of service contract between the user and the websites included an implied right to remove voluntarily

166. *See Commission Proposal*, *supra* note 106, arts. 79(5)(c), (6)(c) (failure to comply with the regulation by any data controller could result in fines up to one million euros or two percent of the operator's annual worldwide income).

167. MAYER-SCHÖNBERGER, *supra* note 12, at 136.

168. *See* RESTATEMENT (SECOND) OF CONTRACTS § 302 (1981).

169. *See* Volokh, *supra* note 72, at 1061 ("Contract law protection . . . . only lets people restrict speech by parties with whom they have a speech-restricting contract, express or implied.").

170. However, a lack of contractual privity would not preclude Nell from pursuing a copyright infringement action against either Marco, myexgirlfriend.com, or any other website that displayed her work without permission.

submitted data, then users would have a viable cause of action against the website operator if the data were not deleted upon request.

However, while an implied covenant requiring data deletion may be read into an agreement between users and website operators, this covenant can be explicitly waived by the parties. 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.[171] As the Court in *Cohen v. Cowles Media* noted, "[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."[172] Thus, while the government may say that Internet terms of service contracts must carry an implied promise that the seller will remove user-submitted data on request, it may not add that this term may not be waived.

The vast majority of website terms of service agreements are "click-wrap" adhesion contracts, and users must accept all the terms offered by the website operator as a condition of using the site—users have no bargaining power to negotiate these terms.[173] Thus, for a website operator to require waiver as a condition of use would eviscerate the user's implied rights of data deletion.[174] "If the right to delete can be waived simply by agreeing to a Web site's Terms of Service, it is likely to have no practical effect whatsoever . . . ."[175] Therefore, even though the government cannot compel website operators to accept a non-waivable right to delete terms, it can require specific, explicit, and informed consent as a precondition to waiver. Further, the government could also provide statutory and extra-legal incentives for companies to voluntarily adopt right to delete terms, such as tax subsidies, safe harbors from vicarious liability,[176] and positive publicity for companies that adopt deletion protocols.

To give data deletion rights weight, statutory damages for the breach of an implied-in-fact data deletion term would need to be

---

171. *See* Cohen v. Cowles Media, 501 U.S. 663, 670–71 (1991); *see also* Volokh, *supra* note 72, at 1061–62.

172. *Cowles Media*, 501 U.S. at 671.

173. An adhesion contract is "a standard-form contract prepared by one party, to be signed by another party in a weaker position, usu[ally] a consumer, who adheres to the contract with little choice about the terms." BLACK'S LAW DICTIONARY 366 (9th ed. 2009). A "click-wrap" or "point and click" agreement is a form of adhesion contract where a computer user assents to the terms of the agreement by clicking a button or ticking a box on a website or other electronic interface.

174. And this would also likely violate the Constitution on First Amendment grounds, as data deletion rights are a sub-species of free speech rights. *See supra* Subpart II.C.

175. Conley, *supra* note 120, at 56.

176. This is similar to those incentives provided to "interactive computer services" and Internet "service providers" under the Communications Decency Act, *see* 47 U.S.C. § 230, or the Digital Millennium Copyright Act, *see* 17 U.S.C. § 512, respectively.

adopted, as providing appropriate relief to aggrieved data subjects would likely prove problematic under common law principles.[177] In general, contract law allows for equitable remedies such as specific performance (here, the deletion of the offending data) only if a court finds monetary damages are not adequate.[178] Likewise, punitive damages are not available for breach of a contract, as they are in tort.[179] Therefore, specific statutory remedies would be required in the form of (a) substantial monetary damages for companies that failed to maintain sufficient data privacy and deletion protocols, and (b) obligatory specific performance of the data deletion term. Also, provisions allowing for the recovery of a prevailing plaintiff's attorney's fees and costs would likely be necessary in order to encourage enforcement of the implied term through litigation.

Finally, additional legislation would be necessary to facilitate pre-filing discovery, as potential plaintiffs currently have no way of knowing whether offending data has actually been removed from defendants' servers.[180] "Possible measures could include shifting the burden of proof from individuals to the information processor, letting criminal rather than civil courts take on enforcement, or lowering court costs to encourage individuals to litigate their information privacy claims."[181]

CONCLUSION

Surprisingly, in the end we come around full circle to *The Right of Privacy*.[182] There, Warren and Brandeis proposed two legal remedies for an invasion of privacy: one based on a breach of confidence, the other on a breach of an implied contract.[183] While the public disclosure tort that grew out of the former strain has withered away from lack of constitutional nourishment,[184] the implied contract branch remains a verdant source for privacy law. As discussed in Part III above, formulating data privacy in terms of implied contractual rights avoids

177. Though the damages it proposed were unrealistically high, as discussed in Subpart II.B., the Commission Proposal may offer some valuable guidance here nevertheless. *See Commission Proposal*, *supra* note 106, at arts. 79(5)(c), (6)(c).

178. *See* RESTATEMENT (SECOND) OF CONTRACTS § 359(1) (1981) ("Specific performance or an injunction will not be ordered if damages would be adequate to protect the expectation interest of the injured party.").

179. *See id.* § 355 ("Punitive damages are not recoverable for a breach of contract unless the conduct constituting the breach is also a tort for which punitive damages are recoverable.").

180. *See, e.g.*, Clayton, *supra* 164.

181. MAYER-SCHÖNBERGER, *supra* note 12, at 139. *See, e.g.*, Council Directive 95/46, art. 23, 1995 O.J. (L 281) 45 (EC).

182. *See* Warren & Brandeis, *supra* note 20, at 211.

183. *Id.*

184. *See supra* Subpart I.C.

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 full measure of the E.C.'s proposal is incompatible with American constitutional and common law principles,[185] a right to delete voluntarily submitted data is legally cognizable.

Legislatively adopting such a right[186] would serve several important public policy goals. First, it would better align corporate data protection practices with users' privacy expectations.[187] Second, it would provide clear guidance to website operators as to what data protocols are legally required, which would allow for more efficient business planning and technology investment. Third, prescribing statutory penalties for failing to comply with these standards would provide a powerful incentive to develop more secure data management technologies and to honor user deletion requests in a timely manner.[188] Fourth, a statutory right of data deletion would potentially help to harmonize data protection policies in the United States and Europe and could possibly forestall the adoption of the more constitutionally troubling aspects of the Committee Proposal.[189] Finally, explicit statutory rights of data privacy would engender greater trust in the marketplace for personal data,[190] allowing individuals to disclose personal data without fear that it will be misused.

Many, if not most, people assume that there are zones of privacy in their lives that are not open for public inspection. In many respects, the default position in the non-digital world is privacy or anonymity, insofar as a person has to take positive steps to be noticed by a larger public. But on much of the Internet, the opposite is true: The default is for personal data to be readily available, and it is only through intentional action that privacy is achieved. Universal access is one of the great virtues of the Internet, but it becomes problematic when people erroneously assume that they have greater privacy online than they actually do. Thus, while there are real risks to free speech implicit in a far-reaching right to be forgotten, the animating spirit of the proposed right—that "[i]f an individual no longer wants his personal data to be . . . stored by a data

185. *See supra* Part II.

186. Under Congress' interstate commerce power. *See* U.S. CONST. art. I, § 8, cl. 3.

187. *See generally* HOOFNAGLE, *supra* 159.

188. While statutory penalties are arguably necessary to ensure compliance by website operators, the amounts stipulated in the Commission Proposal—up to one million euros or two percent of the operator's annual worldwide income—are too high to be realistically enforceable. *See Commission Proposal*, *supra* note 106, arts. 79(5)(c), (6)(c). Further, overly punitive penalties are likely to chill innovation rather than encourage it, as companies will likely become overly cautious in their approach to data management and shy away from developing new technologies, for fear of incurring the regulators' wrath.

189. *See, e.g.*, Rick Mitchell, *Paris Court Says Google Violated 'Right to Forget' of Ex-Porn Actress*, ELEC. COM. & L. REP. (Mar. 23, 2012).

190. *Cf.* Litman, *supra* 138, at 1301–11.

controller, and if there is no legitimate reason for keeping it, the data should be removed"[191]—is worthy of consideration by U.S. legislators and jurists.

191. Reding, Making Europe the Standard Setter, *supra* note 16.