STANFORD TECHNOLOGY LAW REVIEW
VOLUME 16, NUMBER 2 WINTER 2013

IT'S ABOUT TIME: PRIVACY, INFORMATION LIFE CYCLES, AND THE RIGHT TO BE FORGOTTEN

Meg Leta Ambrose*

CITE AS: 16 STAN. TECH. L. REV. 369 (2013)
http://stlr.stanford.edu/pdf/itsabouttime.pdf

ABSTRACT

The current consensus is that information, once online, is there forever. Content permanence has led many European countries, the European Union, and even the United States to establish a right to be forgotten to protect citizens from the shackles of the past presented by the Internet. But, the Internet has not defeated time, and information, like everything, gets old, decays, and dies, even online. Quite the opposite of permanent, the Web cannot be self-preserving. One study from the field of content persistence, a body of research that has been almost wholly overlooked by legal scholars, found that 85% of content disappears in a year and that 59% disappears in a week, signifying a decrease in the lifespan of online content when compared with previous studies.

Those that have debated this privacy issue have consistently done so in terms of permanence and also neglected an important consideration: the changing nature of information over time. Our efforts to address disputes arising from old personal information residing online should focus on the changing value, uses, and needs of information over time and the ethics of preservation. Understanding how information changes over time in relation to its subject, how and where personal information resides online longer than deemed appropriate, and what

* Meg Leta Ambrose is a doctoral candidate in the ATLAS Institute at the University of Colorado, advised by Paul Ohm. She earned her J.D. from the University of Illinois in 2008. She was previously an NSF funded graduate fellow with the University of Colorado Department of Computer Science and research assistant with the Silicon Flatirons Center at the University of Colorado School of Law. She is currently a CableLabs and Harvard Berkman Center for Internet & Society fellow. A special thank you to all those that workshopped this Article at the 2012 Privacy Law Scholars Conference.

information is important for preservation allows regulation to be tailored to the problem, correctly framed. This understanding requires an interdisciplinary approach and the inclusion of research from telecommunications, information theory, information science, behavioral and social sciences, and computer sciences. Recognizing that information does not last forever, this Article takes the initial step of outlining an information life cycle in terms of phases in relation to information needs, creating a taxonomy to help assess the competing values at stake when one seeks to have old personal information "forgotten."

Some of the proposed legislation makes exceptions for historical, statistical, and public safety needs, but none of it includes time, a vital element to the information life cycle. The Article concludes by working through specific issues like revived interest, the integrity and objectivity of the Internet, and the importance of time in protecting the interests other information needs. Permanence is not yet upon us, and therefore, now is the time to develop policies and practices that will support good decisions, preserve our cultural history, and protect the future of the past, as well as protect the privacy rights of individuals that will live with the information and a society that may suffer from the threat of a permanent record.

INTRODUCTION

The prospect of content "adjustment" in the name of privacy has exposed cultural variations on perspectives of the global village.[1] The right to be forgotten has gained traction in Europe as a legal mechanism for handling such information issues and has been named a top priority by the European Commission as it redrafts the 1995 E.U. Data Protection Directive (E.U. Directive).[2] A reaction to the outcry over the permanence of digital information,[3] the right essentially transforms public information into private information upon request of the data subject,[4] also described as "the right to silence on past events in life that are no longer occurring."[5] This concept of oblivion, however, is controversial and has been called "rewriting history," "personal history revisionism," and "censorship" in the U.S. The issues are social, legal, and technical. Because the nature of the Web does not allow us to ignore the impact of the values held by others, oblivion should be considered seriously.

Privacy scholars including Daniel Solove,[6] Viktor Mayer-Schöenberger,[7] Anita Allen,[8] Julie Cohen,[9] Anupam Chander,[10] and Jonathan Zittrain[11] have

---

1. MARSHALL MCLUHAN, THE GUTENBERG GALAXY: THE MAKING OF TYPOGRAPHIC MAN (1962).

2. *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 8, COM (2010) 609 final (Nov. 4, 2010), *available at* http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf [hereinafter *Comprehensive Approach on Personal Data Protection*].

3. *See* Jeffrey Rosen, *The Web Means the End of Forgetting*, N.Y. TIMES, July 21, 2010, http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html; John Hendel, *In Europe, a Right to be Forgotten Trumps the Memory of the Internet*, THE ATLANTIC (Feb. 3, 2011), http://www.theatlantic.com/technology/archive/2011/02/in-europe-a-right-to-be-forgotten-trumps-the-memory-of-the-internet/70643/; *Common Sense with Phineas and Ferb*, THE DISNEY CHANNEL, http://tv.disney.go.com/disneychannel/commonsense/ (last visited Feb. 9, 2013).

4. *Comprehensive Approach on Personal Data Protection*, *supra* note 2. *See also European Commission Sends Draft Regulation Out for Review*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (Dec. 8, 2011), https://www.privacyassociation.org/publications/european_commission_sends_draft_regulation_out_for_review (noting the Right to be Forgotten emphasized information created during childhood and "shall apply especially in relation to personal data which are made available by the data subject while he or she was a child.").

5. Giorgio Pino, *The Right to Personal Identity in Italian Private Law: Constitutional Interpretation and Judge-Made Rights*, *in* THE HARMONIZATION OF PRIVATE LAW IN EUROPE 225, 237 (M. Van Hoecke & F. Osts eds., 2000).

6. *See* DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007).

7. *See* VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE (2009).

8. *See* Anita L. Allen, *Dredging Up the Past: Lifelogging, Memory, and Surveillance*,

investigated the vulnerabilities presented by access to personal information, offering incredible insight into the changes to collection and retrieval of memories, the judgment of others that create real world barriers, and the elimination of second chances. All have embraced permanence – that we cannot be separated from an identifying piece of online information short of a name change. But information persistence research suggests otherwise. This entire field of research is dedicated to measuring how long information remains accessible and unchanged, contributing to bibliometrics and search engine advancements. When articulating the reasons behind the Internet Archive, Brewster Kahle explained the average lifespan of a webpage was around 100 days.[12] In 2000, Junghoo Cho and Hector Garcia-Molina found that 77% of content was still alive after a day,[13] and Brian E. Brewington and George Cybenko estimated that 50% of content was gone after 100 days.[14] In 2003, Dennis Fetterly, et al., found 65% of content alive after a week[15] and in 2004, Alexandros Ntoulas, et al., found only 10% of content alive after a year.[16] Recent work suggests, albeit tentatively, that data is becoming *less* persistent over time; for example, Daniel Gomes and Mario Silva studied the persistence of content between 2006 and 2007 and discovered a rate of only 55% alive after one day, 41% after a week, 23% after 100 days, and 15% after a year.[17] While

---

75 U. CHI. L. REV. 47 (2008).

9. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object,* 52 STAN. L. REV. 1373 (2000).

10. *See* Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* THE OFFENSIVE INTERNET: SPEECH, PRIVACY, AND REPUTATION 124 (Saul Levmore & Martha C. Nussbaum eds., 2010).

11. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 228 (2008).

12. In 1997, Kahle estimated that based on the Internet Archive data, the average URL had a lifespan of 44 days, Brewster Kahle, *Preserving the Internet*, SCIENTIFIC AMERICAN (July 27, 1998), *available at* http://web.archive.org/web/19980627072808/http://www.sciam.com/0397issue/0397kahle.html, and in 2004, the average lifespan of a page was about 100 days, Lisa Rein, *Brewster Kahle on the Internet Archive and People's Technology*, O'REILLY P2P.COM, http://openp2p.com/pub/a/p2p/2004/01/22/kahle.html (last visited Feb. 9, 2013). Today the Frequently Asked Questions section of the site states that the average life of a Web page is 77 days. *Wayback Machine: Frequently Asked Questions,* INTERNET ARCHIVE, http://www.archive.org/about/faqs.php#29 (last visited Feb. 6, 2013).

13. Junghoo Cho & Hector Garcia-Molina, *The Evolution of the Web and Implications for an Incremental Crawler*, PROC. OF THE 26TH INT'L CONF. ON VERY LARGE DATA BASES 200, 200-09 (2000).

14. Brian E. Brewington & George Cybenko, *How Dynamic is the Web?*, 33 COMPUTER NETWORKS 257, 257-76 (2000).

15. Dennis Fetterly, Mark Manasse, Marc Najork & Janet L. Wiener, *A Large-Scale Study of the Evolution of Web Pages*, 34 SOFTWARE PRACTICE AND EXPERIENCE 213, 213-37 (2004).

16. Alexandros Ntoulas, Junghoo Cho & Christopher Olston, *What's New on the Web? The Evolution of the Web from a Search Engine Perspective*, PROC. OF THE 13TH INT'L CONF. ON WORLD WIDE WEB, 1-12 (2004).

17. Daniel Gomes & Mario J. Silva, *Modelling Information Persistence on the Web*,

all of these studies contained various goals, designs, and methods that prevent true synthesis, they all contribute to the well-established principle that the Web is ephemeral,[18] and the average lifespan of content is a matter of days or months at best. The Web cannot be self-preserving.[19]

In an age when "[y]ou are what Google says you are,"[20] expecting parents search prospective names to help their kids retrieve top search results in the future. Only a few rare parents want their children to be "lost in a virtual crowd,"[21] even in light of the notion that "[l]ife, it seems, begins not at birth but with online conception[, a]nd a child's name is the link to that permanent record."[22] Gyslain Raza unwillingly became the Star Wars Kid in 2003, and, according to Google, still is as of 2011. Caitlin Davis was fired and Stacy Snyder was not allowed to graduate for images found on Facebook that offered very little context or truth of their character. Alexandra Wallace quit school and made a public apology for a racist video she posted on YouTube that spurred debate online about a university's authority to monitor or regulate student speech. In 1992, John Venables and Robert Thompson viciously murdered a two-year-old and became the youngest people ever to be incarcerated for murder in English history.

These stories deserve varying levels of sympathy but are all embarrassing, negative, and may lead the subjects to want to disconnect their names from their past transgressions to make them less retrievable when interviewing for a job, college, or first date – *oblivion,* as it is translated from French and Italian.[23] Paradoxically, the only individuals who have been offered oblivion are the two who committed the most heinous social offense: Venables and Thompson were given new identities upon their release from juvenile incarceration.[24] It may actually be easier for two convicted murderers to get a job than Alexandra Wallace.

This paradox is one of many that result from an inconsistent and distorted conception of information persistence and how to manage it in the Internet Age. One problem with new forms of access to old information is that without

---

PROC. OF THE 6TH INT'L CONF. ON WEB ENGINEERING 193, 193 (2006).

18. Wallace Koehler, *A Longitudinal Study of Web Pages continued: A Consideration of Document Persistence*, 9 INFO. RES. 1 (2004), available at http://informationr.net/ir/9-2/paper174.html.

19. JULIEN MASANÈS, WEB ARCHIVING 7 (2006).

20. Megan Angelo, *You Are What Google Says You Are*, WIRED.COM (Feb. 11, 2009), http://www.wired.com/epicenter/2009/02/you-are-what-go/.

21. Allen Salkin, *What's in a Name? Ask Google*, N.Y. TIMES, Nov. 25, 2011, http://www.nytimes.com/2011/11/27/fashion/google-searches-help-parents-narrow-down-baby-names.html.

22. *Id.*

23. The right to oblivion, or the French "droit à l'oubli" and Italian "diritto al' oblio."

24. Jamie Doward, *James Bulger Killer Jon Venables Confessed Real Identity to Strangers As Mental State Crumbled*, THE OBSERVER, Mar. 6, 2010, http://www.guardian.co.uk/uk/2010/mar/07/jon-venables-confessed-identity.

rhyme or reason much of it disappears while pieces of harmful content remain. Another is that damaging personal information that an individual could have previously moved on from lingers, creating a disproportionate harm. Time disrupts the information system and information values upon which U.S. information privacy law has been based, and so we must reassess our views and practices in light of this disruption. Objections to the preservation of personal information may be valid; when content has aged it becomes increasingly uncontextualized, poorly duplicated, irrelevant, and/or inaccurate, a process I call the information life cycle.

Old personal information has never been the problem it threatens to be in the Internet Age – old information threatens harsh and wide-reaching consequences to the socially valued and often protected individual interests of reputation, identity, and rehabilitation. The law is ill-equipped to handle this problem and scholars have been dismissive of proposed solutions. In order to properly manage the value and harms of old information, it is appropriate to analyze how time impacts information generally, on the Web, and future information behavior, yet this research has not been fully considered thus far in privacy law scholarship. Balancing information needs requires more rigor and input from the social, information, and computer science.

Undertaking an interdisciplinary approach to the problem, this Article will first, in Part I, argue that the law is currently ill-equipped to embrace the changing value of information over time, explore contextual integrity as an avenue for conceptualizing old information and privacy violations, introduce proposed right to be forgotten legislation, and objections to the right. Part II outlines two social movements related to Web content persistence, digital forgetting and digital preservation. Information persistence research suggests that we have missed something – Web content is fleeting and requires maintenance to remain accessible, resulting in a great deal of disappearing information. With this in mind, Part III will lay a foundation for a more nuanced approach to considering old information (the information life cycle), offer a preliminary assessment of how information transforms over time in relation to two categories of information needs, and set forth scenarios to represent each type of relevant information circumstances. Finally, Part IV addresses the language of the proposed legislation, accounting for the objections in Part I, and gives a partial defense of the language and the way in which it acknowledges some aspects of the information life cycle – thus having minimal potential impact on other information users, while protecting the privacy of individual users. However, there is an important missing element: time.

I. OLD INFORMATION, PRIVACY, AND THE LAW

The law is currently in no shape to handle information that has been properly disclosed but becomes harmful and devalued. Information privacy is an evolving concept and access to old personal information may be a privacy

violation or form of information injustice. The novel idea proposed by the right to be forgotten is that in the newly forming Information Society one should hold the right to have personal information migrate from a public or disclosed sphere to a private or limited access sphere after a period of time. Adapting the right to the Digital Age is controversial and not without obstacles. This Part introduces the relationship between the law, privacy, the right to be forgotten, and articulated objections.

A. *Fitting Old Information into the Existing Model of Privacy*

There are four principle legal mechanisms utilized by those who want to control or limit the flow of information about them once it is released: intellectual property restrictions,[25] contractual obligations,[26] defamation,[27] and the privacy torts ((1) intrusion upon seclusion; (2) public disclosure of private facts; (3) misappropriation; (4) false light).[28] Copyright is very useful for preventing the replication of content created by the information subject, but only reaches the creative aspects of that work and does not reach information created by another related to the subject.[29] Contractual obligations only restrain those who are privy to the contract, and so much of the information disclosed about an individual is outside of this tool.[30] Defamation creates a cause of action to protect one's reputation from false claims, as long as the individual is not a public figure or limited purpose public figure.[31] Intrusion upon seclusion protects one from the "intentional invasion of solitude or seclusion of another through either physical or nonphysical means such as eavesdropping, peeping through windows or surreptitiously opening another's mail."[32] The public disclosure of private facts is a cause of action against one who disseminates generally unknown private information, even if it is true.[33] One may also be sued for using another's name, likeness, or other personal attributes without permission for exploitative purposes, or misappropriation.[34] In states that

---

25. Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop Others from Speaking About You*, 52 STAN. L. REV. 1049 (2000).

26. *See* Cohen v. Cowles Media Co., 501 U.S. 663 (1991) (holding that contracts not to speak are enforceable and do not violate the First Amendment).

27. RODNEY A. SMOLLA, LAW OF DEFAMATION (2d ed. 1999).

28. William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

29. Volokh, *supra* note 25.

30. *See Cohen*, 501 U.S. 663 (holding that contracts not to speak are enforceable and do not violate the First Amendment).

31. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 279-80 (1964); Time, Inc. v. Firestone, 424 U.S. 448, 451-58 (1976).

32. RODNEY A. SMOLLA, SMOLLA AND NIMMER ON FREEDOM OF SPEECH §24:1 (2010).

33. Samantha Barbas, *The Death of the Public Disclosure Tort: A Historical Perspective*, 22 YALE J.L. & HUMAN. 171, 172-77 (2010).

34. Prosser, *supra* note 29.

recognize it, a claim for false light can be brought if a defendant publishes information that places the subject in a highly offensive light.[35] This claim addresses false impressions as opposed to false statements.[36]

The difference between the above information disputes and those related to oblivion is that there is nothing necessarily illegal or undesirable about the information when it is initially collected or published online. The difference is time. The right to oblivion addresses information that may be outdated, irrelevant, harmful, and/or inaccurate. This information haunts the individual, causing undesirable repercussions for the subject, as well as society which may be chilled by the prospect of permanence.

The privacy torts, many of which are not relevant to oblivion as they address false or undisclosed information, have been significantly restricted to protect free speech. Definitions of privacy range from the right to be left alone[37] to an essential aspect of self-determination.[38] As a natural right it has been described as the "inalienable right of the individual to hold inviolate the fortress of self."[39] The right to privacy crafted by the Supreme Court in 1965 in *Griswold v. Connecticut* serves only to protect against an overbearing and too powerful government, offering no protection against private intrusion.[40] Any protection, therefore, is derived from a matter of common or statutory law. The conflict between expression and privacy is inevitably lopsided as one of Constitutional versus common or statutory law. The values of privacy and the First Amendment have been balanced and lines have been drawn between negligence and actual malice,[41] public figures and private citizens,[42] and public concerns and private interests[43] to guide lower courts. The attempts by judges, legislators, and advocates to etch out some space for privacy concerns in light of the reverence for expression, explicitly granted in the Constitution, has been woefully unsuccessful.

While expression is generally and feverishly protected, categories of speech have been exempted from protection because of their low value – undeserving of protection.[44] These categories are obscenities, threatening

---

35. Diane Leenheer Zimmerman, *False Light Invasion of Privacy: The Light that Failed*, 64 N.Y.U. L. REV. 364, 374 (1989).

36. Prosser, *supra* note 29.

37. Introduced by Judge T. Cooley in 1888 and popularized by Samuel D. Warren and Louis D. Brandeis in *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

38. ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967).

39. WILLIAM H. MARNELL, THE RIGHT TO KNOW: MEDIA AND THE COMMON GOOD 145 (1973).

40. 381 U.S. 479, 484 (1965).

41. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 283-88 (1964).

42. *See* Curtis Publ'g v. Butts; Associated Press v. Walker, 388 U.S. 130, 154-55 (1967).

43. *See* Rosenbloom v. Metromedia, Inc., 403 U.S. 29, 39-56 (1971).

44. Cass R. Sunstein, *Low Value Speech Revisited*, 83 NW. U. L. REV. 555 (1989).

words, fighting words, incitement, fraud, and child pornography.[45] Because information value changes over time, it may become more difficult to prioritize the value of expression and access of such information over the harms to dignity, privacy, and reputation suffered by the subject.

Public interest is built into information disputes through the protection of "newsworthy" content or content that "the public has a proper interest in learning about."[46] In 1967, the U.S. Supreme Court recognized newsworthiness as defense to privacy claims involving true disclosures in *Time, Inc. v. Hill*, declaring that privacy must yield "in a society which places a primary value on freedom of speech and of press."[47] In *Cox Broadcasting Corp. v. Cohn*, the Court decided that truthful publication of a rape victim's name obtained from public records was Constitutionally protected.[48] A similar set of facts led to the same result in *Florida Star v. B.J.F.*, in which the Court narrowly decided the issue of whether information obtained from the public domain – subsequently published by the press – created liability under the public disclosure tort favorably for the press.[49] Generally, the right to know trumps privacy harms.

While U.S. law is not yet prepared to address old, truthful, harmful information, it has implicitly recognized the impact of time on information, the information life cycle outlined in Part III. Upon its release, the heightened protection from the First Amendment protects information over other rights, values, and interests. When pitted against privacy at this stage, newly distributed information claims many more wins than losses.

Courts define prior restraint as "a predetermined judicial prohibition restraining specific expression."[50] A heavy presumption of invalidity follows any requirement of judicial approval prior to publication. The presumption originated in 1931 in *Near v. Minnesota* when Chief Justice Hughes reversed a trial court's injunction on *The Saturday Press* pursuant to a Minnesota law based on public nuisance:

> The fact that the liberty of the press may be abused by miscreant purveyors of scandal does not make any the less necessary the immunity of the press from previous restraint in dealing with official misconduct. Subsequent punishment for such abuses as many exist is the appropriate remedy, consistent with constitutional privilege.[51]

Thus, the government "carries a heavy burden of showing justification for the imposition of such a restraint."[52] The Pentagon Papers case fumbled over the exceptions described in *Near* when the Supreme Court rejected an

45. Ashcroft v. Free Speech Coal., 535 U.S. 234, 246 (2002).
46. RESTATEMENT (SECOND) OF TORTS § 652D cmt. d (2012).
47. 385 U.S. 374, 388 (1967).
48. 420 U.S. 469, 486-96 (1975).
49. 491 U.S. 524, 541 (1989).
50. Chi. Council of Lawyers v. Bauer, 522 F.2d 242, 248 (7th Cir. 1975).
51. 283 U.S. 697, 632 (1931).
52. Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971).

Executive-sought injunction to prevent the *New York Times* and *Washington Post* from publishing classified information related to the Vietnam War – information previously undisclosed, despite being dated.[53] Justices Black and Douglas made no exception for national security, Justice Brennan allowed for injunctions only during war time, Justices Stewart and White required proof that the Nation would suffer "direct, immediate, and irreparable damage,"[54] and Justice Marshall stressed the absence of legislation guiding the Court.[55] Even when dealing with old information, the presumption against prior restraints can only be overcome by an extreme danger to national security or some overriding governmental interest.

Regulation may be slightly easier to swallow once information is no longer newsworthy. Attorney, health, financial, personnel, government, and library records are regulated. These records are considered private in nature, and dissemination by those responsible for their care is punishable under certain circumstances. These are examples of government bodies in the U.S. outlining life cycles for records based on their value. Statutes of limitations are particularly relevant. These statutes acknowledge the injustices that can result from utilizing old information with diminishing reliability over time and "founded upon the liberal theory that prosecutions should not be allowed to ferment endlessly in the files of the government to explode only after witnesses and proofs necessary to the protection of the accused have by sheer lapse of time passed beyond availability."[56]

The law has also recognized the end of the information lifecycle in rare circumstances. Statutory protections and judicial practices have embraced an expiration phase[57] for the availability and use of certain information. A court may be petitioned to seal or expunge criminal records of a juvenile.[58] The Fair Credit Reporting Act generally disallows the use of information older than seven years that may cast the consumer in negative or unfavorable light.[59] While it may be naïve, the hope is that the information no longer represents the individual and would limit her opportunities if it were attached to her name as

53. *See* N.Y. Times Co. v. United States, 403 U.S. 713, 714, 724 (1971).

54. *Id.* at 730.

55. *Id.* at 733.

56. United States v. Eliopoulos, 45 F. Supp. 777, 781 (D.N.J. 1942).

57. For a more thorough discussion of these protections and practices *see* Meg Leta Ambrose, Nicole Friess & Jill Van Matre, *Seeking Digital Redemption: The Future of Forgiveness in the Internet Age*, 29 SANTA CLARA COMPUTER & HIGH TECH. L.J. 99 (2012).

58. Aidan R. Gough, *The Expungement of Adjudication Records of Juvenile and Adult Offenders: A Problem of Status*, 1966 WASH. U. L. REV. 147, 162 (1966).

59. 15 U.S.C. § 1681a(f) (2012); *see* Equifax Inc. v. Fed. Trade Comm'n, 678 F.2d 1047, 1050 (11th Cir. 1982) (defining "adverse information" as "information which may have, or may reasonably be expected to have, an unfavorable bearing on a consumer's eligibility or qualifications for credit, insurance, employment, or other benefit, including information which may result, or which may be reasonably expected to result, in a denial of or increased costs for such benefits.").

she moves through life.[60]

Although the law may acknowledge certain aspects of aging information, the single publication rule is the best example of an unwillingness to reassess information over its life cycle. Under this rule, even when a defamatory mass communication reaches multiple people, it gives rise to only one action for libel.[61] The point is to avoid "multiplicity of actions; to protect the defendant from excessive liability based on single publication run; to allow the plaintiff to recover all of his damages at once; and to reduce the chilling effect that the common-law rule might have on the mass communication of ideas."[62] The Supreme Court, however, has also stated that limited restrictions on free speech would "invite timidity and self-censorship and very likely lead to suppression of many items that would otherwise be published and that should be available to the public."[63] These are, of course, the concerns with the retention of and easy access to old information, but the law has not developed a system for weighing the competing values at issue with old information.

B. *Fitting Old Information into a New Model of Privacy*

One model for assessing privacy violations is Helen Nissenbaums's contextual integrity.[64] Nissenbaum outlined a privacy framework based on expected information flows, called contextual integrity.[65] When the flow of information adheres to established norms, the unsettling emotions of a privacy violation rarely occur.[66] When the flow of information does not meet the expectations, a violation has occurred and contextual integrity has not been maintained.[67] Borrowing a term from Jeroen van den Hoven, information may be placed in a particular 'sphere of access' that prevents 'informational injustice.'[68] Van den Hoven explains, "What is often seen as a violation of privacy is often more adequately construed as the morally inappropriate transfer of personal data across the boundaries of what we intuitively think of as separate 'spheres of justice' or 'spheres of access'."[69]

To help determine whether information access represents a privacy violation, the information flow can be cross-referenced with its life cycle phase.

---

60. Ambrose, Friess & Van Matre, *supra* note 57, at 122-49.

61. Lori A. Wood, *Cyber-Defamation and the Single Publication Rule*, 81 B. U. L. Rev. 895, 913 (2001).

62. Salyer v. S. Poverty Law Ctr., 701 F. Supp. 2d 912, 914 (2009).

63. *Cox Broad.*, 420 U.S. at 496.

64. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004).

65. *Id*. at 129-57.

66. *Id*.

67. *Id.*

68. JEROEN VAN DEN HOVEN & JOHN WECKERT, INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY 314 (2008).

69. *Id*.

If the information is accessible in a specific phase such that access violates the expected or accepted information flow, a privacy violation has occurred. The information is sitting in the incorrect sphere of access. Previously, simple access to old information about an individual was restricted to information that was recently distributed and a limited time thereafter. In contrast, Facebook's Timeline is an example of easier access to old information that disrupts the expected information flow that causes the unsettling effect of a privacy violation.[70] If access to aged information continues in a way that disrupts contextual integrity, restrictions to the information can be developed to limit access or use to those that need the information.

To identify when information may be moved into a different sphere of access to maintain contextual integrity, Part III creates an initial taxonomy for determining the life cycle phase for each piece of information in relation to the information needs and use that exist at each phase. Identifying the relevant needs and information life cycle phase in the scenarios helps to determine whether a privacy violation has occurred and whether it should be moved to a different sphere of access based on its specific information uses and values. Information should reside in its appropriate sphere at each phase of its life cycle in order to protect the subject and the integrity of the information. Data managers and Internet users should consider themselves responsible for maintaining spheres of access to information under their control. The more difficult question is whether we are willing to move information into its appropriate sphere of access when a privacy violation has been identified – necessarily complicating access by the public. There are growing legislative efforts that suggest we may be willing to move information into different spheres of access.

C. *Proposed Legislation*

The right to be forgotten has a long history in the analog world. Its adaptation to the Digital Age and incorporation into the E.U. General Data Protection Regulation ("E.U. Regulation"), the updates to the E.U. Directive, is complicated because many information practices have changed since 1995. Much of the E.U. Directive must be completely reconsidered and lines redrawn.

The right to be forgotten has been conceived as a legal right and as a value or interest worthy of legal protection,[71] as well as a virtue,[72] social value,[73] and

---

70. *Public Opinion Rejects Facebook Timeline [Infographic]*, SODAHEAD (Feb. 03, 2012), http://www.sodahead.com/united-states/public-opinion-rejects-facebook-timeline-infographic/question-2429779/.

71. Antoinette Rouvroy, *Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?*, *in* LA SÉCURITÉ DE L'INDIVIDU NUMÉRISÉ. RÉFLEXIONS PROSPECTIVES ET INTERNATIONALES 249-78 (Stéphanie Lacour ed., 2008), *available at* http://works.bepress.com/antoinette_rouvroy/5.

72. MAYER-SCHÖNBERGER, *supra* note 7.

ethical principle.[74] The right has been categorized as a privacy claim even though it applies to information that is, at least to some degree, public. It represents an attempt to migrate personal information from a public sphere to a private sphere. Being forgotten (the right to have third parties forget your past) and forgetting (the right to avoid being confronted with your own past) are embraced by the French concept of *oubli*, or oblivion, and denotes a negative right that others abstain from remembering one's past, as well as a subjective right of the individual to control his past and future.[75]

Legal action to force forgetfulness is not novel; in fact, European Commissioner Viviane Reding stated that the E.U. Regulation would *clarify* the right to be forgotten in 2010.[76] German[77] and Swiss[78] legal systems are instances of the clean slate interpretation and embrace a notion of oblivion in which an individual may preclude another from identifying him in relation to his criminal past. Digital oblivion was introduced in 2010 as a legislative project in France, which was intended to force third parties to delete information after a period of time or upon request of a user. It represents the erasure concept.[79] The charter was signed by a number of actors which did not include Google or Facebook.[80] The Italian Data Protection agency found

---

73. Jean-Francois Blancette & Deborah G. Johnson, *Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness*, 18 THE INFORMATION SOCIETY 33-45 (1998).

74. Martin Dodge & Rob Kitchin, *'Outlines of a world coming into existence': Pervasive computing and the ethics of forgetting*, 34 ENVIRONMENT AND PLANNING B: PLANNING AND DESIGN 431-45 (2007).

75. Rouvroy, *supra* note 71.

76. At that point in 2010, the closest approximation was defined as "the right of individuals to have their data fully removed when they are no longer needed for the purposes for which they were collected or when he or she withdraws consent or when the storage period consented to has expired." *Comprehensive Approach on Personal Data Protection*, *supra* note 2.

77. The German right to personality protects individual privacy from true, non-defamatory statements found in Art. 2.1 of the Basic Law of Germany. Beyond the offense details and prosecution of the case, the right limits coverage of the individual in relation to the crime after time has passed. *See* Judgment of June 5, 1973 (Lebach I), Bundesverfassungsgericht [BVerfG], Entscheidungen des Bundesverfassungegerichts [BVerfG] (decisions of the federal constitutional court) 35, 202, English synopsis available at http://www.law.ed.ac.uk/ahrc/personality/gercases.asp#Lebach.

78. *See* Franco Werro, *The Right to Inform v. the Right to be Forgotten: A Transatlantic Clash*, *in* LIABILITY IN THE THIRD MILLENNIUM; GEORGETOWN PUBLIC LAW RESEARCH PAPER NO. 2 285-300 (A. Colombi Ciacchi, C Godt, P Rott, & LJ Smith eds., 2009), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1401357.

79. *French Government Secures 'Right to be Forgotten' on the Internet*, Privacy and Information Security Law Blog, Hunton & Williams LLP, (Oct. 21, 2009) http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/.

80. *Comments of the European Consumers' Organisation (BEUC) to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union* (Jan. 24, 2011), http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en

similar legal obligations in Article 11 of its data protection legislation.[81] The Spanish Data Protection Agency has certainly gained the most U.S. attention by bringing suit against Google to remove URLs from its index that point to personal information the Agency has determined appropriately forgotten.[82] The dispute involves information like a notice of home repossession for non-payment of social security and a reference to a plastic surgeon's alleged botched operation that settled out of court; both are information produced and maintained by traditional news sources and retrieved by Google's search engine when the individuals' names are entered.[83] Google appealed five of the determinations to the Audiencia Nacional, which in turn referred it to the Court of Justice of the European Court of Justice for clarification.[84]

The E.U. Charter of Fundamental Rights of the European Union grants that "everyone has the right to the protection of personal data concerning him or her" and that "such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[85] And finally, "everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified."[86] The erasure of data finds further elaboration in the '95 E.U. Directive in art. 14 which grants the data subject a general right to object on compelling legitimate grounds to the processing of his data, with limitations,[87] and in art. 6(1)(e) which requires personally identifiable information be kept no longer than necessary for the purposes it was collected.[88]

The proposed language related to the right to be forgotten in the E.U. Regulation has evolved since 2010. Reding declared the right to be forgotten to be a pillar of the new E.U. Regulation,[89] but its formulation has been controversial. Today, as it is written into the proposed E.U. Regulation, the

---

.pdf.

81. Pere S. Castellano, *The Right to be Forgotten Under European Law: A Constitutional Debate*, 16 LEX ELECTRONICA 1 (2012).

82. Suzanne Daley, *On Its Own, Europe Backs Web Privacy Fights*, N.Y. TIMES, Aug. 9, 2011, http://www.nytimes.com/2011/08/10/world/europe/10spain.html?pagewanted=all&_r=0.

83. Claire Davenport, *Spain Refers Google Privacy Complaints to EU's Top Court*, REUTERS (Mar. 2, 2012), http://www.reuters.com/article/2012/03/02/eu-google-idUSL5E8E230020120302?feedType=RSS&feedName=vcMedia&virtualBrandChannel=10109&utm_source=dlvr.it&utm_medium=twitter&dlvrit=59213.

84. *Id*.

85. Charter of the Fundamental Rights of the European Union, para. 1 (OJ C 364/1 of 18.12.2000).

86. *Id*.

87. Council Directive 95/46/EC, art. 14, 1995 O.J. (L281) 13 (EU).

88. Council Directive 95/46/EC, art. 6(1)(e), 1995 O.J. (L281) 10 (EU).

89. Viviane Reding, Vice-President, European Comm'n, Your Data, Your Rights: Safeguarding Your Privacy in a Connected World Privacy Platform, The Review of the E.U. Data Protection Framework (Mar. 16, 2011), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183.

right to be forgotten means a data subject has the right that their personal data are erased and no longer processed, where:

a) the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed,
b) where data subjects have withdrawn their consent for processing or when the storage period consented to has expired, and there is no other legal ground for processing the data;
c) the data subject objects to the processing of personal data where they object to the processing of personal data concerning them or the processing of the data does not comply with the Regulation for other reasons.[90]

This right is imposed against a data controller, defined as " the natural or legal person, public authority, agency or any other body which. . . determines the purposes, conditions and means of the processing of personal data."[91] The definition means that *everyone* is potentially a data controller, including the site operator (whether it's Facebook or your personal blog), users that post on sites, and intermediaries.[92]

Exceptions to the right to be forgotten include:

a) exercising the right of freedom of expression;
b) reasons of public interest in the area of public health;
c) historical, statistical and scientific research purposes;
d) compliance with legal obligation to retain personal data; and
e) restricted processing of personal data where the accuracy is contested, the purposes of proof, processing is unlawful and the data subject requests restriction instead of erasure, or the data subject requests the data be transmitted into another automated processing system.[93]

Paragraph 2 of art. 17 also explains that personal data made public can be erased and that the data controller will be responsible for communicating erasure requests to downstream processors.[94] Jeffrey Rosen has pointed out that this right does not necessarily apply only to information produced by the subject, because personal data is defined as "any information relating to a data subject."[95]

---

90. *Commission Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, art. 17(1), at 51. COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [hereinafter *Proposed Data Protection Regulation*].

91. *Id.* art. 5(5), at 41.

92. *See* Rebecca Wong, *The Social Networking: Anybody is a Data Controller*, SOCIAL SCIENCE RESEARCH NETWORK (2008), http://ssrn.com/abstract=1271668.

93. *Proposed Data Protection Regulation*, *supra* note 90, art. 17(3), (4), at 52.

94. *Id.* art. 17(2), at 51.

95. Jeffrey Rosen, *The Right to be Forgotten*, 64 STAN. L. REV. ONLINE 88, 89 (2012).

The right to be forgotten is not exclusively a European notion. At least not when it comes to children. Congress designated children and teens as needing particular attention on this issue.[96] The right to be forgotten is the "right to develop" according to Congressman Markey, author of the Do Not Track Kids Act, designed to update the Children's Online Privacy Protection Act.[97] He has insisted that we must "free the future selves" of children.[98] Markey proposed to require the operator of a website, online service, online application, or mobile application "to the extent technologically feasible, to implement mechanisms that permit users of the website, service, or application of the operator to erase or otherwise eliminate content that is publicly available through the website, service, or application and contains or displays personal information of children or minors," also known as the "eraser button."[99] He stated that "kids should have a right to be forgotten" but also that the right is for everyone; children fifteen and under need to be immediately protected and are the best place to start.[100] As the right moves forward, its definition and scope need thoughtful input from researchers.

Generically, the right to be forgotten "is based on the autonomy of an individual becoming a rightholder in respect of personal information on a time scale; the longer the origin of the information goes back, the more likely personal interests prevail over public interests."[101] These proposals focus on the individual rights that remain with a piece of information after it leaves the individual's control, but whether the issues are privacy, proprietarily, or contractually grounded and whether forgetting is a data subject's right or a data processor's obligation has muddied an effective approach to the problem of old information. Assuming the development of some form of control to remain with the subject of the information, information needs and value will need to be assessed to meet the privacy concerns of the subject and the access concerns of the public. The remainder of the Article organizes the issues and offers rhetoric to analyze the issues and attributes of old information. Any sort of regulation must closely analyze old information and its changing values to appropriately weigh it with competing needs and values.

---

96. *See European Commission Sends Draft Regulation Out for Review*, *supra* note 4; Edward J. Markey, *Children and Teen Online Privacy*, http://markey.house.gov/issues/children-and-teen-online-privacy.

97. Edward J. Markey, *EU Conference: Privacy and Protection of Personal Data, United States Institute of Peace*, YOUTUBE (Mar. 19, 2012), http://www.youtube.com/watch?v=mdD07BVBZbo.

98. *Id*.

99. Do Not Track Kids Act, H.R. 1895, 112th Leg., 1st Spec. Sess. § 7(b)(1)(A), at 24 (Ma. 2011), *available at* http://markey.house.gov/sites/markey.house.gov/files/documents/dntk_legislation_0.pdf.

100. Markey, *supra* note 97.

101. Rolf H. Weber, *The Right to be Forgotten: More than a Pandora's Box?*, 2 JIPITEC 120, 121 (2011), available at http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf.

D. *Objections*

The right to be forgotten raised eyebrows in the U.S. when two German murderers, Wolfgang Werlé and Manfred Lauber, released after serving their time in prison, utilized the right to suppress their names from a number of websites including Wikipedia.[102] Werlé and Lauber attempted to do the same for the English language Wikipedia entry by sending a cease and desist letter to the Wikimedia Foundation,[103] explaining that "[Werlé's] rehabilitation and his future life outside the prison system is severely impacted by your unwillingness to anonymize any articles dealing with the murder."[104] The Electronic Frontier Foundation rebutted the argument: "At stake is the integrity of history itself."[105] The right to be forgotten does not have a concise definition but generally empowers individuals to access and delete personal data collected by third parties, as well as limit access to information from one's past published on the Web under certain circumstances. Some of the objections to the right to be forgotten are briefly discussed here and again in Part IV in relation to suggested changes to the right to be forgotten language in the proposed E.U. Regulation.

There is some general consensus between the U.S. and the E.U. regarding citizens' rights related to the access and control of data collected and stored by companies (erasure).[106] There is a larger divide on the second concept — whether one can limit access to personal information of the past accessible online that causes harm to the subject (oblivion). Other authors have found it important to distinguish these two concepts when supporting one and not the other. The Center for Democracy and Technology has explained that the difference between oblivion and erasure is that of "passive or transactional data sharing – when a service collects and uses personal data in the context of a commercial transaction, [versus] active or expressive data sharing – when content is authored or disseminated by users themselves."[107] Proponents of this

---

102. Some decisions were overturned by Higher Regional courts which allowed for the matter to be heard by the German Federal Court of Justice. *See* Bundesgerichtshof [BGH] [Federal Court of Justice], No. VI ZR 346/09 (Feb. 1, 2011) (faz.net); BGH, No. VI ZR 114/09 (Feb. 1, 2011) (sz-online.de); BGH, No. VI ZR 245/08 & 246/06 (Apr. 10, 2010) (morgenweb.de); BGH, No. VI ZR 227/08 & 228/08 (Dec. 15, 2009) (Deutschlandradio); BGH, No. VI ZR 217/08 (Nov. 2009) (rainbow.at).

103. *Cease-and-desist Letter on Behalf of Mr. Wolfgang Werlé to the Wikimedia Foundation*, Inc., WIRED (Oct. 27, 2009), http://www.wired.com/images_blogs/threatlevel/2009/11/stopp.pdf.

104. *Id*.

105. Jennifer Granick, *Convicted Murderer to Wikipedia: Shhh!* DEEPLINKS BLOG (Nov. 10, 2009), https://www.eff.org/deeplinks/2009/11/murderer-wikipedia-shhh.

106. This has been called "mostly symbolic and entirely unobjectionable" by Rosen, *supra* note 95, at 90.

107. *Comments of the Center for Democracy & Technology to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union*, CTR. FOR DEMOCRACY & TECH. (Jan. 15, 2011), https://www.cdt.org/files/pdfs/CDT_DPD_Comments.pdf.

right describe it as "a way to give (back) individuals control over their personal data and make the consent regime more effective," limiting the right to be forgotten to "data-processing situations where the individual has given his or her consent."[108] Paul Bernal has argued that the right to be forgotten needs to be renamed and recast as a right to delete, stating "the default should be that data can be deleted, and that those holding the data should need to justify why they hold it."[109] Granting a right to delete essentially adds a caveat to contract law, allowing the user to reassess the consent she has given. The goal is to give more control to the user over his or her data. The right to be forgotten known as digital oblivion is one motivated by the need to offer opportunity for one to move beyond her past, easily accessible to others online. The right to be forgotten may mean anything along a spectrum, including: a right to delete data held by sites and data brokers (arguably information created by the system, not the user), a right to delete information they themselves have authored and posted (possibly including the reposting of the information by another user), and/or the right to delete information drafted by another. Any lines that can be drawn between the two concepts will continue to blur, and the E.U. Regulation refers to data being "made public" by a data controller and that third parties processing the data must be informed.[110] This language suggests no such distinction is intended. The goals of each are actually more similar than they seem at first glance; both to seek to remove limitations created by personal information from the past and must be balanced with other information needs. This objection is reconsidered further in Part IV(D).

The most obvious objection is that the right to be forgotten violates freedom of expression, because it would allow the user to limit the speech of others about her. Jeffrey Rosen has articulated this point, arguing that "[a]lthough there are proposals in Europe and around the world . . . that would allow us to escape our past, these rights pose grave threats to free speech."[111] He cautions that "[u]nless the right is defined more precisely when it is promulgated over the next year or so, it could precipitate a dramatic clash between European and American conceptions of the proper balance between privacy and free speech, leading to a far less open Internet."[112] Eugene Volokh has also argued that Google's search results are protected speech.[113] However,

---

108. Jef Ausloos, *The 'Right to be Forgotten' – Worth Remembering?,* 28 COMPUTER L.& SECURITY REV. 143, 143 (2012).

109. Paul A. Bernal, *A Right to Delete?*, 2 EUR. J.L. & TECH. 2 (2011), http://ejlt.org/article/view/75/144.

110. *Proposed Data Protection Regulation*, *supra* note 90, art. 9(2), at 46.

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

112. Rosen, *supra* note 95, at 88.

113. Eugene Volokh & Donald M. Falk, *Google: First Amendment Protection for Search Engine Search Results*, GOOGLE WHITE PAPER (Apr. 20, 2012), http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf.

the Supreme Court has recognized individual privacy interests in information that was once public but may have been "wholly forgotten."[114] "Otherwise private information may have been at one time or in some way in the 'public domain,' does not mean that a person irretrievably loses his or her privacy interests in it."[115] That "an event is not wholly 'private' does not mean that an individual has no interest in limiting disclosure or dissemination of the information."[116] This objection is discussion further in Part IV(C).

Finally, Vint Cerf has criticized the right to be forgotten as unachievable stating, "You can't go out and remove content from everybody's computer just because you want the world to forget about something."[117] While the right to be forgotten does not suggest removing files from personal computers, Cerf's point highlights that "forgetting" must necessarily mean degrees of accessibility. People may remember very shameful actions far longer than their current laptop will last, the topic of Part II to follow. This was the context of Cerf's comment, the opening of the new Life Online Gallery at Bradford's National Media Museum which preserves aspects of digital life that are not often collected. Cerf is terrified when he conjures up the analogue equivalent to the right to be forgotten. Limited accessibility of analogue paper information prevented the harm addressed by the right to be forgotten — a great deal of "forgetting" occurred on its own. Documents and books with little ongoing interest are often very difficult to find over time. For instance, if only one person has checked a text out from a library thirty years ago, it is likely not to survive the next round of collection management scrutiny. This objection is discussed further in Part IV(B).

II. CONTENT PERSISTENCE ON THE WEB

> "You can define a net in one of two ways, depending on your point of view. Normally, you would say that it is a meshed instrument designed to catch fish. But you could, with no great injury to logic, reverse the image and define a net

---

The paper was drafted in response to anti-competitive business practices, but the implications of First Amendment protection for this type of automatically generated search result information is relevant to this debate. The Spanish Data Protection Agency has resorted to ordering Google to remove results when traditional news sources have rejected the Agency's request to alter the content it has determined should be forgotten. Limiting a search engines ability to prefer its own products and services in search results is not the same as the forced removal of sites from its index, but Volokh argues that Google's aggregation of materials authored by others, search results presented to users, and editorial choices are protected by the First Amendment.

114. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 769-70 (1989).

115. Halloran v. Veterans Admin., 874 F.2d 315, 322 (5th Cir. 1989).

116. *Reporters Comm*., 489 U.S. at 770 (citation omitted).

117. Matt Warman, *Vint Cerf Attacks European Internet Policy*, TELEGRAPH (Mar. 29, 2012), http://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html.

> as a jocular lexicographer once did: he called it a collection of holes tied together with string."
> Julian Barnes, *Flaurbert's Parrot*

All information has value — to someone, under some circumstances, at some time. All information has no value — to someone, under some circumstances, at some time. The right-to-be-forgotten debate has to this point assumed that all information is permanently accessible, but this misconception suggests that information retains its value over time. The complication is that information removal can be just as dangerous as information storage; the nuances of how information changes over time are insightful to policy that seeks to protect privacy with little impact on other information users. The information relevant to the rest of the discussion is digital, identifying, and easily retrievable. It does not address paper records or deep Web content. In the Internet age, how can we preserve information that may be important later in an easily accessible form while still providing individuals with the ability to move on from their pasts and giving society the peace of mind that comes from forgetting and forgiving?

Consider two movements related to the persistence of Web content, both covered by the mainstream media. The first movement occurred at the turn of the century, in the late 1990s, when Brewster Kahle, famed computer scientist, network engineer, and digital librarian, warned that the Web's future could be similar to the lost Library of Alexandria if measures like the Internet Archive were not taken.[118] The second movement occurred about ten years later and voiced the polar opposite of Brewster's concern. In July, 2010, *The Web Means the End of Forgetting* by Jeffrey Rosen was published by the New York Times.[119] In it Rosen asks how we can "best . . . live our lives in a world where the Internet records everything and forgets nothing — where every online photo, status update, Twitter post and blog entry by and about us can be stored forever."[120] The Disney Channel runs PSAs directed at children reminding to "be careful what you put online; it never goes away, ever!"[121] In October 2010, regulatory reaction to the second concern was being seriously considered in France,[122] and in November 2010, for the entire E.U.[123] If this aspect of the

118. Rick Weiss, *On the Web, Research Work Proves Ephemeral*, WASH. POST, Nov. 24, 2003, http://faculty.missouri.edu/~glaserr/205f03/Article_WebPub.html.

119. Rosen, *supra* note 3.

120. *Id*.

121. *Common Sense with Phineas and Ferb*, *supra* note 3.

122. HUNTON & WILLIAMS LLP, *French Government Secures 'Right to be Forgotten' on the Internet*, PRIVACY AND INFO. SECURITY L. BLOG (Oct. 21, 2010), http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/.

123. *Communication from the Commission to the European Parliament, the Council, The Economic and Social Committee on the Regions, A Comprehensive Approach on Personal Data Protection in the European Union*, EUROPEAN COMM'N, Nov. 4, 2010,

Web is to be regulated, we must understand the extent of the harms caused and tailor any limitations on access to content to those sources that truly last beyond their utility.

A. *Digital Ephemerality*

"Good words do not last long unless they amount to something."
Niimiipu Chief Joseph, Washington, D.C., 1879

"The Internet is a moving target. Every minute, thousands of Web pages are updated or abandoned."[124] This was the headline of an article in *Slate* magazine from 1997. There may be nothing less natural than permanence. The Web, of course, is not really permanent. Or as Kahle explains, "of course, the Internet is quite fleeting."[125] On the one hand, fourteen years later, I find the articles cited readily accessible online. On the other hand, who knows how many more sources there once were?

As early as 1985, those concerned with preservation were readying the troops creating reports, conferences, and strategies to handle this new electronic "crisis."[126] That year the Committee on the Records of Government proclaimed, "The United States is in danger of losing its memory."[127] And over a decade later, the term "digital dark ages" was coined at a 1997 conference of the International Federation of Library Associations and Institutions.[128] In 1998, a collection of librarians, archivists, and computer scientists joined for a project, "Time and Bits: Managing Digital Continuity," the proceedings of which were collected, posted online, and disappeared within a year.[129] "Digital documents last forever — or five years, whichever comes first," joked computer scientist Jeff Rothenberg, in 1998.[130]

Digital librarians seek to maximize access to the cultural treasures of their society once reserved for only a few as well as collect our born-digital cultural representations. "Culture, any culture. . . depends on the quality of its record of knowledge."[131] Today, records of knowledge depend not on brittle papyrus or

---

available at http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

124. Bill Barnes, *Nothing but Net*, SLATE (Feb. 28, 1997), http://www.slate.com/articles/technology/webhead/1997/02/nothing_but_net.html.

125. Rein, *supra* note 12.

126. ROY ROSENZWEIG, CLIO WIRED: THE FUTURE OF THE PAST IN THE DIGITAL AGE 8 (2011).

127. *Id*.

128. Terry Kuny, *A Digital Dark Ages? Challenges in the Preservation of Electronic Information*, 63RD INT'L FED'N OF LIBRARY ASS'NS AND INSTS. (IFLA) COUNCIL AND GEN. CONFERENCE (Sept. 4, 1997), available at http://archive.ifla.org/IV/ifla63/63kuny1.pdf.

129. ROSENZWEIG, *supra* note 126.

130. JEFF ROTHENBERG, AVOIDING TECHNOLOGICAL QUICKSAND 2 (1998).

131. Donald J. Waters, *Digital Archiving: The Report of the CPA/RLG Task Force*, *in*

the acid decay of paper, but the "death of the digit."[132] Generally, the problem is two-fold. First, technology advances so rapidly that the time before a technology becomes obsolete is decreasing. Second, digital resources are less stable than their analog counterparts resulting in the corruption of the integrity and authenticity of the resource.[133]

> The most vexing problems of digital media are the flipside of their greatest virtues. Because digital data are in the simple lingua franca of bits, of ones and zeros, they can be embodied in magnetic impulses that require almost no physical space, be transmitted over long distances, and represent very different objects . . . But the ones and zeros lack intrinsic meaning without software and hardware, which constantly change because of technological innovation and competitive market forces.[134]

A laundry list of errors prevent long-term access to digital content: media and hardware errors, software failures, communication channel errors, network service failures, component obsolescence, operator errors, natural disasters, internal and external attacks, and economic and organizational failures.[135] An endeavor to preserve the 1960 U.S. Census data provides a good example of the basic issue. It was widely spread that computers could no longer read the data, but by 1979 the Census Bureau had transferred almost all (1,575 records were lost to deterioration) of the records to newer compatible tapes.[136] While persistence is not impossible, it is a major engineering effort. Kevin Kelly, co-founder of *Wired*, explained, "The Internet is basically the largest Xerox machine in the world. If something can be copied it will be copied. On the Internet, it goes everywhere. But what it doesn't do is it doesn't go forward in time very well."[137]

In 1997, Kahle estimated that based on the Internet Archive data, the average URL had a lifespan of 44 days[138] and in 2004, the average lifespan of a

---

PRESERVATION AND DIGITISATION: PRINCIPLES, PRACTICES AND POLICIES, NAT'L PRESERVATION OFF. ANN. CONF., at 39 (Sept. 3-5, 1996), *available at* http://www.bl.uk/blpac/pdf/conf1996.pdf.

132. Bernard Frischer points out that a DigiCult document (www.digicult.info/downloads/ html/6/6-212.html) misattributed this phrase to Mary Feeney's THE DIGITAL CULTURE: MAXIMISING THE NATION'S INVESTMENT (1999). Bernard Frischer, *New Directions for Cultural Virtual Reality: A Global Strategy for Archiving, Serving, and Exhibiting 3d Computer Models of Cultural Heritage Sites*, PROC. OF THE CONF., VIRTUAL RETROSPECT, at 175 n.33 (Nov. 8-9, 2005).

133. *The DigiCULT Report: Technological Landscapes for Tomorrow's Cultural Economy – Unlocking the Value of Cultural Heritage*, EUROPEAN COMMISSION DIRECTORATE-GENERAL FOR THE INFORMATION SOCIETY 210 (2002), *available at* http://www.digicult.info/pages/report2002/dc_fullreport_230602_screen.pdf.

134. ROSENZWEIG, *supra* note 126, at 9.

135. HENRY M. GLADNEY, PRESERVING DIGITAL INFORMATION 10 (2007).

136. ROSENZWEIG, *supra* note 126, at 8.

137. MARGARET MACLEAN & BEN H. DAVIS, TIME & BITS: MANAGING DIGITAL CONTINUITY 6 (1998).

138. Kahle, *supra* note 12.

page is about 100 days.[139] The Frequently Asked Questions section of the site today states that the average life of a Web page is 77 days.[140] This ephemerality has continued to motivate digital preservationists and archivists to create management tools to locate and preserve content before it is gone. It also has motivated computer scientists to measure and understand Web persistence. The following are a number of studies done on the subject.

"The World Wide Web still is not a library,"[141] stated Wallace Koehler in the last of a three-sequence study published in 2004 that tracked URLs since 1996. "It is well established that Web documents are ephemeral in nature."[142] He measures persistence in terms of half-lives, "that period of time required for half of a defined Web literature to disappear."[143] A number of studies were being produced that had shorter timelines. These studies questioned printed Internet guides and Web resources,[144] one finding an attrition rate of 28% and 50% over two and three year periods.[145] Others concerned themselves with URL citations in scholarship, measuring the methods increased use and declining viability. Citations in legal scholarship that were tested in mid-2001 produced the following results: 39% dated 2001 failed, 37% dated 2000 failed, 58% of those dated 1999 failed, 66% dated 1998 and 70% dated 1997 failed.[146] When URLs fail as access points to content they have suffered "linkrot." Much of the persistent Web that does not suffer from linkrot are navigation pages (those that serve to guide the user though a site), as opposed to content pages (pages providing information.)[147] In 2003, two-thirds of the original sample, which was about half navigation and half content pages, were gone, and three-quarters of pages that remained were navigation pages.[148] Koehler notes that there is a steady state after rapid decline in URL linkrot and that more research needs to be done on resource lifetimes.[149]

---

139. Rein, *supra* note 12.

140. *Wayback Machine: Frequently Asked Questions,* INTERNET ARCHIVE, http://www.archive.org/about/faqs.php#29 (last visited Feb. 6, 2013).

141. Koehler, *supra* note 18.

142. *Id*.

143. *Id*.

144. Carol Anne Germain, *URLs: Uniform Resource Locators or Unreliable Resource Locators* 60 C. AND RES. LIBR. 359 (2000); Mei Kobayashi & Koichi Takeda, *Information Retrieval on the Web*, 32 ACM COMPUTING SURVEYS 144 (2000); Mary K. Taylor & Diane Hudson, *"Linkrot" and the Usefulness of Web Site Bibliographies* 39 REFERENCE & USER SERVICES Q. 273 (2000).

145. S. Mary P. Benhow, *File not found: The problem of changing URLs for the World Wide Web*, 8 INTERNET RES.: NETWORK APPLICATIONS AND POL'Y 247, 248 (1998).

146. Mary Rumsey, *Runaway Train: Problems of Permanence, Accessibility, and Stability in the Use of Web Resources in Law Review Citations*, 94 LAW LIBR. J. 27, 35 (2002).

147. Koehler, *supra* note 18, at 5.

148. *Id.*

149. *Id*.

A study by Cho and Garcia-Molina downloaded 720,000 pages from "popular" web servers daily for four months to study whether the document had changed.[150] More than 20% of pages changed between each crawl (daily); more than 40% of .com pages changed daily, but less than 10% of .edu and .gov pages changed daily.[151] It took 50 days for 50% of the web to change or be replaced by new pages.[152] Brewington and Cybenko built a web clipping service that collected about 100,000 pages per day from March and November, 1999.[153] 56% of pages did not change over the duration of the study while 4% changed every single crawl.[154] Another study that crawled 151 million pages once a week for eleven weeks attempted to measure frequency and degree of change and found that most changes were minor modifications.[155]

"Despite the ephemeral nature of the web, there is persistent information."[156] Research done more recently, collected data between 2003 and 2006, by Gomes and Silva measured the lifetime of URLs and content, as well as synthesized and compared their findings to previous works.[157] They found that of the fifty-one million pages harvested from the Portuguese national community web URLs had a half-life of two months and a site half-life of 556 days.[158] The most common reasons for URL death are replacement or recycling of URLs and site death.[159] The half-life for content was two days.[160] These findings suggest a decreased lifetime of content when compared with previous studies, visualized in Figure 1.[161] Figure 2 extends the rate of disappearance found to project the point at which none of the originally collected information would remain, which is approximately 8.42 years. According to this body of research, around 10% to 15% of content persists after a year.[162] Additionally, research on the stability of search results over time finds that approximately 90% of the 12,600 queries collected have their top ten results altered within a ten day period.[163] Kahle concluded, "It's a huge problem . . . This is no way to run a culture."[164]

---

150. Cho & Garcia-Molina, *supra* note 13, at 200-09.
151. *Id*. at 205.
152. *Id*. at 208.
153. Brewington & Cybenko, *supra* note 14, at 258-59.
154. *Id*. at 261.
155. Fetterly et al., *supra* note 15, at 213-37.
156. Gomes & Silva, *supra* note 17, at 193.
157. *Id.*
158. *Id*. at 195.
159. *Id*. at 194-95.
160. *Id*. at 196-97.
161. *Id*.
162. *Id*. at 199.
163. Jinyoung Kim & Viktor R. Carvalho, *An Analysis of Time Stability in Web Search Results*, PROC. OF THE 33RD EUROPEAN CONF. ON ADVANCES IN INFO. RETRIEVAL 466-78 (2011).
164. Weiss, *supra* note 118.

FIGURE 1. CONTENT LIFESPAN REDUCED BY 34% BETWEEN STUDIES, BASED ON GOMES AND SILVIA (2006).

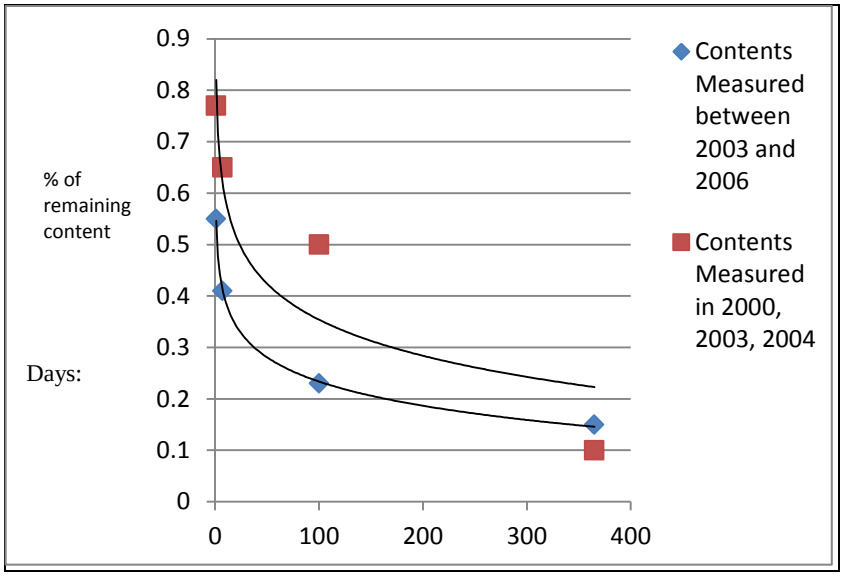
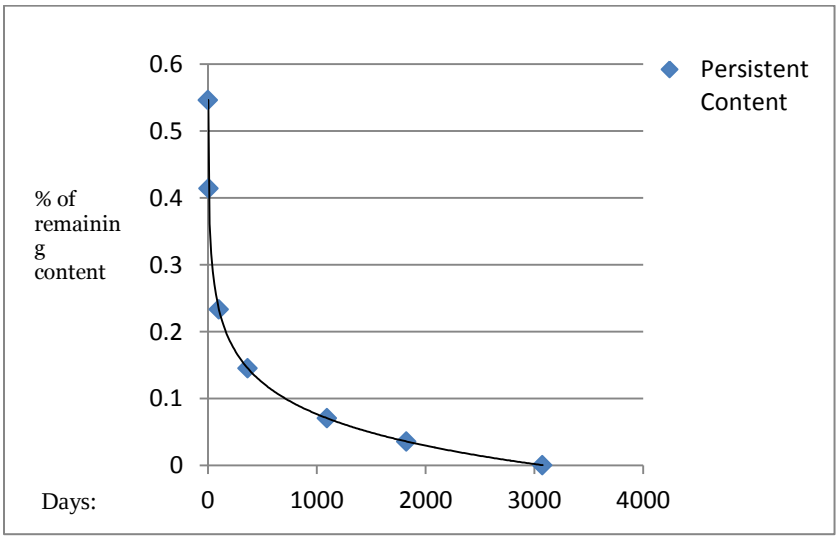


FIGURE 2. PROJECTED 8.42 YEARS FOR ALL CONTENT PERSISTENCE TO REACH ZERO, BASED ON GOMES AND SILVIA (2006).



"If we are to understand the dynamics of the Web as a repository of

knowledge and culture, we must monitor the way in which that knowledge and culture is managed. We find that the Web in its 'native form' is a far too transitory medium,"[165] stated Koehler before insisting that initiatives like Internet Archive are vital. Kahle set out four questions related to his goal of making all published works accessible to everyone in the world: "Should we do this? Can we do this? May we do this? And will we do this?"[166] He answers the first question "as almost a postulate of yes"[167] and explains that he and this perspective are "very American."[168] Kahle acknowledged in his first major publication on the project that there are serious privacy concerns with Internet Archive.[169] These two principles, access and privacy, have come to a head as the threat of access to harmful information is the debate of the day.

B. *Digital Permanence*

> "Nothing fixes a thing so intensely in memory as the wish to forget it."
> Michel De Montaigne

In the movie *The Social Network*, Mark Zuckerberg's ex-girlfriend explains to him that "[t]he Internet isn't written in pencil, it's written in ink."[170] Google CEO Eric Schmidt quipped that "every young person. . . will be entitled automatically to change his or her name on reaching adulthood in order to disown youthful hijinks stored on their friends' social media sites."[171] The joke was taken seriously by Jonathan Zittrain who foresees a "whole-person" reputation rating system developing and promotes a system of "reputation bankruptcy."[172] Similarly, John Hendel explains that "[w]e live naked on the Internet. . . in a brave new world where our data lives forever."[173] French President Nicolas Sarkozy has declared, "Regulating the Internet to correct the excesses and abuses that come from the total absence of rules is a moral imperative!"[174]

As noted above, in 1990 Werlé and Lauber brutally murdered actor Walter

---

165. Koehler, *supra* note 18.

166. Stuart I. Feldman, *A Conversation with Brewster Kahle*, 2 QUEUE 24, 26 (June 2004), *available at*http://delivery.acm.org/10.1145/1020000/1016993/interview.pdf?ip=24.8.100.220&acc=OPEN&CFID=74082650&CFTOKEN=17740014&__acm__=1324244873_8fe5f34cbb620770199ba6a2f0b0e59d.

167. *Id*.

168. *Id*.

169. Kahle, *supra* note 12.

171. THE SOCIAL NETWORK (Columbia Pictures 2010).

171. Holman W. Jenkins, Jr., *Google and the Search for the Future*, WALL ST. J., Aug. 14, 2010, http://online.wsj.com/article/SB10001424052748704901104575423294099527212.html (quoting Google CEO Eric Schmidt).

172. ZITTRAIN, *supra* note 11, at 228.

173. Hendel, *supra* note 3.

174. *Id.*

Sedlmayr. The conviction is a matter of public record and, because of the actor's fame, a Wikipedia entry. In Fall 2009, a cease and desist letter was sent to Wikipedia demanding the name of one of the guilty parties be removed from the site citing German law that protects the name and likeness of a private person from unwanted publicity.[175] Likewise, Switzerland recognizes a general right to personality that has interpreted privacy rights to protect criminals that have served their time.[176] When media outlets move their records online and maintain an Internet archive, this right may be infringed. In 2009, France gave the concept a name "le Doit a l'Oubli" which translates as "the Right to Oblivion." The campaign, led by French Secretary of State heading developments in the digital economy Nathalie Kosciusko-Morizet, drafted codes of conduct, one for behavioral advertising and one for social networks and search engines, to be signed by industry members.[177]

Spain has now taken up shaping the right to be forgotten, backed by over 80% of its population.[178] More than 90 citizens filed formal complaints with the Spanish Data Protection Agency, among them a domestic violence victim's address and an old college arrest.[179] After assessing the privacy concerns of each complaint and failing to persuade the source of the content to take action, the Agency ordered Google to stop indexing the information. Google challenged the order saying that editing the index "would have a profound chilling effect on free expression without protecting people's privacy"[180] and would violate the "objectivity" of the Internet.[181]

Two authors that agree on the future of forgetting, but see the issue differently, are Gordon Bell and Viktor Mayer-Schönberger. In *Total Recall*, Bell celebrates the e-memory revolution[182] and Mayer-Schönberger is concerned about the chilling effects that will be created by "perfect remembering."[183] Mayer-Schönberger convincingly describes in great length

---

175. Cease-and-desist Letter on Behalf of Mr. Wolfgang Werlé to the Wikimedia Foundation, *supra* note 103. This case is discussed in more detail in Part IV.

176. Werro, *supra* note 78.

177. HUNTON & WILLIAMS LLP, *French Government Secures 'Right to be Forgotten' on the Internet*, PRIVACY AND INFO. SECURITY L. BLOG (Oct. 21, 2010), http://www.huntonprivacyblog.com/2010/10/articles/french-government-secures-right-to-be-forgotten-on-the-internet/.

178. José Luis Rodriguez, Director of the Spanish Data Protection Agency, Address at the 33rd International Conference of Data Protection and Privacy Commissioners (Nov. 2, 2011).

179. Daley, *supra* note 82.

180. *Id*.

181. Elizabeth Flock, *Should We Have a Right to be Forgotten Online?*, WASH. POST , Apr. 20, 2011, http://www.washingtonpost.com/blogs/blogpost/post/should-we-have-a-right-to-be-forgotten-online/2011/04/20/AF2iOPCE_blog.html.

182. GORDON BELL & JIM GEMMEL, TOTAL RECALL: HOW THE E-MEMORY REVOLUTION WILL CHANGE EVERYTHING (2009).

183. MAYER-SCHÖNBERGER, *supra* note 7, at 5.

the advances in storage capacity and the ease with which storage of everything could in fact be possible, and Bell describes his e-memory vision as inevitable. "I am a technologist, not a Luddite, so I'll leave abstract discussions about whether we should turn back the clock to others. Total Recall is inevitable regardless of such discussions."[184] Digital information is superior "because it lacks the noise problem," states Mayer-Schönberger, referring to Claude Shannon's theory of noise: decay with use, time, and reproduction.[185] Bell prefers digital memory because it is "objective, dispassionate, prosaic, and unforgivingly accurate."[186]

But, digital content cannot be detached from its physical mediums; it cannot be impervious to decay. Such a quality is not, as of today, part of any record system; space, time, and energy are limitations nothing can escape. Additionally, content on the Internet is and has been easily editable, leaving no residue from the pen or pencil; the problem described above by archivists and historians. In fact, the tools used in *The Social Network* to injure the ego of Zuckerberg's ex-girlfriend allowed for easy erasure.[187]

C. *Preservationists vs. Deletionists*

These movements have produced two camps: Preservationists and Deletionists. Preservationists believe we owe the entire Internet to our descendants.[188] Deletionists believe forgetting must be part of the Internet to support efficient, useful, and high quality information practices.[189] As the above discussion outlines, it is *possible* that content can be easily accessible for a very long time, but permanence does not, at this point, appear to be a pervasive threat to most. Additionally, these two movements remind us that the Web is very young and has transformed greatly in the last 10 years. It may be that these harms are not pervasive enough to regulate, can be managed by other means, or do not justify a manipulation of the Web as it is still transitioning. Or one may perceive this aspect of the Web as a very good reason to allow individuals to be forgotten; after all, much of the Web disappears. Why not offer oblivion to those hurt by rare instances of content persistence that includes the subject's name? While these normative questions will remain unanswered throughout this Article, the above discussion provides a broader

184. BELL & GEMMEL, *supra* note 182, at 159.

185. MAYER-SCHÖNBERGER, *supra* note 7, at 57.

186. BELL & GEMMEL, *supra* note 182, at 56.

187. Although similar to a blogging program, after the movie's success the old "online diary" was dug up and can be found at http://www.scribd.com/doc/538697/Mark-Zuckerbergs-Online-Diary.

188. Sumit Paul-Choudhury, *Digital Legacy: The Fate of Your Online Soul*, NEWSCIENTIST (May 2, 2011), http://www.newscientist.com/article/mg21028091.400-digital-legacy-the-fate-of-your-online-soul.html.

189. *Id*.

perspective of time's impact on Web content and the issue of forgetting. One may find the right to be forgotten more or less justified after the discussion, but time's impact on networked information should be understood (more so than it is) if regulation is to be crafted at its least intrusive. The above movements represent the dramatic reactions people have to long-term concerns regarding the Internet. These concerns stem from the human impacts of loss or preservation of information, based on technological realities – expiration of technological functionality vs. ease of storage and retrieval.

So, *some* information lasts *longer* than the information subject, and possibly society, deems appropriate. Although a great deal of embarrassing information may make its way online, it will not necessarily remain accessible long enough to qualify for oblivion, depending on the form it takes. Searching for "Kayla Laws" today does not retrieve the same results that it did when the notorious "revenge porn" site IsAnybodyUp.com was in operation.[190] The site, which invited users to post "pornographic souvenirs from relationships gone sour," folded on April 19, 2012 and now redirects users to BullyVille.com, an anti-bullying website.[191] Laws was one of the few individuals that spoke out as a victim of the site, being interviewed by Nightline.[192] The only reference to the content related to her on IsAnyoneUp.com is found on the second page of Google results in one or two news stories about the site's end. JuicyCampus.com, a site that targeted college students and encouraged them to post content which was often malicious and pornographic, shut down in 2009 citing the declining economy and falling ad revenue.[193] Based on the reasons for disappearing data we can assume certain things about that which will remain longer. Information will remain with entities that have the resources to and interest in maintaining access to information as it ages. For instance, searching for "Alexandra Wallace" today on Google retrieves traditional news sources and Perez Hilton. While search results will vary due to personalization, Google Trends shows that interest in Alexandra Wallace only existed for a matter of weeks in 2011.[194]

These nuances matter, because a balanced approach to old information must account for the nature of information – time changes that nature. The risks are too high to mis- or over-regulate this issue. Regulation should be tightly tailored and the information issue must be accurately stated to do so. More detailed research on content persistence is necessary to understand exactly what

---

190. Lee Moran & Beth Stebner, *Now FBI launch investigation into founder of 'revenge porn' site Is Anyone Up?*, DAILY MAIL (May 23, 2012), http://www.dailymail.co.uk/news/article-2148522/Hunter-Moore-founder-revenge-porn-site-Is-Anyone-Up-investigated-FBI.html.

191. *Id*.

192. *Id*.

193. *College gossip website shuts down, citing economy*, USA TODAY (Feb. 5, 2009), http://www.usatoday.com/tech/webguide/internetlife/2009-02-05-juicycampus_N.htm.

194. *See* Figure 4 below.

could and should be regulated. Because information requires care in order to remain accessible on the Web, both goals set forth by the above movements require some type of action. To determine what type of action should be taken toward old information, before rights or obligations can be created, we need a structure for thinking about old information that embraces all of the various information circumstances that arise. The remainder of this Article attempts to draw lines and categorize information needs and stages of information aging in order to incorporate these nuances into the proposed legislation.

D. *Addressing the New Problem of Old Information*

Whether a Preservationist or Deletionist, the above persistence research shows that intervention is necessary to promote either perspective; a lack of intervention represents another perspective in and of it itself. While all information that lands online will not remain there forever, more information finds itself online and may land on a site that maintains its content for a very long time. This information may be truly harmful to reputation and identity, but also may (have) create(d) a norm of non-disclosure that negatively impacts society on a larger scale. The engagement in self-presentation, according to David Velleman, is what it means to be a person. "The person conceives of himself as dynamic and as trying to improve himself morally."[195] Just the threat of digital permanence may prevent what John Stuart Mill called "experiments in living."[196] Without control of self-presentation and room for experimentation, moral autonomy suffers.[197]

In order to prevent this type of self-stagnation, limiting access to or deleting personal information from the past has been proposed. Combating permanent information with a right to delete results in take it or leave it options for policy-makers – they must choose to either support access and expression or privacy and reinvention. Instead, I suggest a more nuanced analysis of old information. Determining whether self-stagnation harms caused by access to personal information, or a lack of control over the flow of personal information, outweigh the value of the aged information requires a closer look at how information changes.

All information is not created equal, and even if it is, it does not remain equal. Different information has different value and that value changes as time passes. The desire to move forward without being shackled to one's past may result in information disputes with the information creator, storer, and

---

195. VAN DEN HOVEN, *supra* note 68, at 319.

196. 18 JOHN STUART MILL, *On Liberty*, *in* COLLECTED WORKS OF J.S. MILL 213, 260-67 (J.M. Robson ed., 1977).

197. *See* Jeroen van den Hoven, *Information Technology, Privacy, and the Protection of Personal Data*, *in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY, 301, 315-16 (Jeroen van den Hoven & John Weckert eds., 2008).

intermediaries. All information disputes weigh competing rights, values, and/or interests to determine the best course of action for a specific type of information (true, false, newsworthy, owned, private, etc.). Disputes related to old information are no different, but require a reassessment of information characteristics and valuation under the conditions of passed time. As information ages it takes on new characteristics relevant to its role in meeting the needs of society. These nuances matter to crafting appropriately tailored policy. By first clearly delineating information conditions, Part III describes how adding attributes of age to an information condition supports appropriate, nuanced consideration of the value of old information so that it can be weighed with competing interests more accurately.

III. OLD INFORMATION: A LIFE CYCLE PERSPECTIVE

> "Myth, memory, history – these are three alternative ways to capture and account for an elusive past, each with its own persuasive claim."
>
> Warren I. Susman

This Part analyzes the value of a single piece of information as it meets the needs of the present and the future. It may be helpful to think about information as a single file – a representation or piece of communication. When confronted with an old piece of personal information, the question "why should this information be retained?" can and should be asked. The following offers a more structured response to this question. The information in each of the six scenarios below will meet different needs as the information ages. In light of these changing values, the harms may become injustices. By determining the needs at issue and how personal information meets those needs over its lifetime, informed decisions can be made regarding old information.

A. *Oblivion Scenarios*

An effective approach to old information requires a closer look at the balance that must be struck between harms to the subject and benefits of access. The current approach of "keep it or delete it" allows only one side to win, but preventing self-stagnation and access to information are two important social goals that can be protected if the nuances of old information are teased out. Acknowledging these nuances allows policymakers to create balanced and tailored regulation. There are a number of scenarios that the right to be forgotten may reach; the differences in these scenarios should not be ignored because they may prevent opportunities to achieve the goals of privacy and preservation. The value of information varies over time, which should not be ignored for the same reason. In order to ground the issues expressed above and assess contested aspects of access intervention throughout the remainder of the paper, I offer six scenarios as an attempt to represent each type of information scenario that may arise:

(1) A Facebook image from a user's college days portraying a camping trip where she went skinny-dipping five years ago (actively created by the subject on the initial site it was posted); (2) a rape victim whose name was included in a news story from ten years ago about the rape allegations and conviction (actively created content by someone other than the subject, on the initial site); (3) information on the child support owed by a father that washes downstream to a "dead beat dad" site and resides there years after all payments have been made and a relationship has been built with the child (actively created content by another residing downstream); (4) a young user's racist tweet about her favorite young adult movie adaptation that has been retweeted throughout the Twittersphere that is now seven years old (actively created content by the subject that has been moved downstream from the initial site); (5) the passively created data that is collected by an initial site, e.g., Amazon (passively created data, subject-derived, held by the initial site); and (6) traded to another, e.g., Acxiom (passively created, subject-derived, downstream). Assume that the subject has a strong desire to limit access to this information to alleviate the harms easy access continues to cause.

The right to be forgotten may cover all of these scenarios that vary dramatically in almost every way (resides on initial or downstream location, created by the subject or another, is passively or actively created). If the right does not impact actively created content, it would not reach scenarios one through four because they are authored as opposed to passively collected data (a blurry distinction). If the right applies only to information that the subject creates either passively or actively, it would apply to the information held by Amazon, Acxiom, Facebook, and possibly Twitter, but not the news or busted.com. If the right does not extend beyond its criminal past roots, only busted.com would be limited in publishing the information. The right to be forgotten may play out in a number of different ways depending on how the E.U. Regulation and other laws shake out. Part III offers a structure for categorizing information in terms of life cycle phases to assist in addressing how information should be managed as it ages to meet a number of demands.

The issues that arise from information related to one's past must be addressed by policy makers as they consider the future of the past and the privacy concerns of their constituents. But, the future of the past is not going to hinge on decisions related to the permanent record accumulating from the beginning and end of our entire existence, as it has been described in relation to this problem elsewhere. The future of the past will hinge on political, legal, technological, and social considerations of the impact and value of old information.

B. *Information Needs*

Information, like privacy and any other closely analyzed term, suffers from a contentious definition. Claude Shannon's work spawned the field of information theory and a less axiomatic definition of the term information.[198] Information in the formal, engineering sense, developed by Shannon, is a quantitative description of the output of an information source.[199] Shannon ignored the meaning held by the information, or as Leon Brillouin stated, ignores "the human value of the information."[200] This Article must consider information as content, having meaning, because it deals with competing human values associated with the human-created/processed information. The rich debate on the definition of information is beyond the scope of this Article. However, Wersig offers six types of information: structures of the world are information; knowledge developed from perception is information; message is information; meaning assigned to data is information; effect on a specific process is information; and process or transfer is information.[201] For the purposes of this Article, information will have two broad meanings, a condensed version of Wersig's set. The first uses information as an action word, to inform or communicate. The second is a noun, that which represents something in the world; an opinion, fact, idea represented by language, image, numbers, etc. This simplified definition becomes useful when assessing the value of information at each phase of its life cycle.

Within the IT community, information life cycle management is "the policy-driven management of information as it changes value through the full range of its life cycle from conception to disposition."[202] Information takes on different values over its life cycle depending on whether the information need is immediate or remote. Information for immediate purposes involves that which is relevant to immediate decisions based on the current state of the world. Information for remote purposes is that which is relevant to uncovering previously unknown insight into the past or future. These categories of information needs help us to better assess our competing demands of aged information and remind us that management principles from other disciplines have provided groundwork for these issues. For each life cycle phase presented below, the immediate and remote needs of information users must be considered and, as discussed in the final section, acknowledged and protected by information privacy legislation.

---

198. Rafael Capurro & Birger Hjorland, *The Concept of Information*, 37 ANN. REV. OF INFO. SCI. AND TECH. 343, 358-59 (2003).

199. *Id.* at 360-61.

200. LEON BRILLOUIN, SCIENCE AND INFORMATION THEORY, at x-xi (2d ed. 1962).

201. Gernot Wersig, *Information Theory*, *in* INTERNATIONAL ENCYCLOPEDIA OF INFORMATION AND LIBRARY SCIENCE 312-13 (J. Feather & P. Sturges eds., 2003).

202. DAVID G. HILL, DATA PROTECTION: GOVERNANCE, RISK MANAGEMENT, AND COMPLIANCE 57 (2009).

1. *Immediate Needs*

While the value of information is subjective, it can be assigned objective value when it is an action potentially influenced by the information, and the consequences of the action can be measured on some scale of value.[203] Immediate needs are the need for information to make decisions, and the value of information is its role in maximizing expected utility.[204] Information, then, is assessed based on its utility value. An IT professional manages information over its life cycle for the utility purpose of a single entity.

There are certain principles of information that make its valuation a unique assessment for immediate information needs. Unlike almost all other resources or properties that have characteristics of divisibility, appropriability, scarcity, and decreasing returns on use, information is the opposite.[205] Information is infinitely shareable – I can possess it while you possess it and a million others possess it. In fact, shared information, or increased information use, increases its value. Unused information is arguably not information at all. It requires human interaction and more people utilizing the information to maximize its value. The more information is used, the more information is created—it is self-generative, a concept that squarely contradicts general principles of other resources. New or consequential information is produced from many individuals processing information. The value of information, therefore, also increases when combined with other information.

Similar to other resources, however, information is perishable. Its value depreciates over time.[206] Different types of information depreciate in value more quickly than others. This generally correlates to the relevance and accuracy of content. Information, as a representation of something in the world, will not be relevant or accurate forever and maybe not for long. The shape of Earth, stock prices, lyrics to a song, and addresses all have different rates at which their relevancy and accuracy will diminish. In turn, the value of the information record will diminish.

Finally, while the value of information increases upon combination, it does not necessarily increase upon accumulation. Humans seek more information beyond the threshold of optimal cognitive processing. Information behavior studies show that individuals gain increased confidence and satisfaction in decisions made with excess information, but poorer performance rates.[207]

---

203. DAVID G. LUENBERGER, INFORMATION SCIENCE 130 (2006).

204. *Id*.

205. Rashi H. Glazer, *Measuring the Value of Information: The Information-Intensive Organization*, 32 IBM SYSTEMS JOURNAL 99, 101 (1993).

206. *Id*.

207. *See* Michael J. Driver & Theodore J. Mock, *Human Information Processing Decision Style Theory, and Accounting Information Systems*, 50 ACCT. REV. 490 (1975); Jacob Jakoby, Donald E. Speller & Carol A. Kohn, *Brand Choice as a Function of Information Overload: Replication and Extension*, 1(1) J. CONSUMER RES. 33-42 (1974);

The immediate needs for the six scenarios include decision-making needs related to the individual based on the current state of the subject and information currently representing the individual. When it was created, the skinny dipping image may have been very relevant to hiring or dating decisions as well as news reporting. The rape victim story may have been relevant to many immediate decisions, such as which neighborhoods to avoid. The inclusion of the victim's name may have been relevant to many decisions made about her, such as employment or relationships, but allowing use of this information for immediate decisions is not socially desirable. The information about the dead beat dad was likely to be relevant to the school his child attended when trying to meet his or her educational needs, or to a woman deciding whether or not to say yes to his marriage proposal. The racist tweets may have been very relevant to immediate decisions that involve the teen's character, intelligence, and maturity, such as college admissions, dating, befriending, and work. The data scenarios (those passively created and derived from the data subject) may have immediate information needs related to how to meet the needs of the customer, like mailing a product to the correct address or providing desired services. Access to information for immediate needs is imperative to complete specific tasks of a particular entity, but information may meet the needs of non-specific tasks as well.

2. *Remote Needs*

Beyond immediate decision-making needs, aged information not only helps us learn about and from our past, it also helps us make better decisions about the future. While the benefits of targeted advertising may be disputable outside of the marketing industry, predictive analytics also claim a benefit to fraud prevention, data security, health care, and machine learning – that we can better understand our world by analyzing all of this information.[208] Remote informational needs have a long history of safeguards elsewhere. For instance, academic researchers involved with human subjects are guided by a set of ethical principles enforced by Internal Review Boards and commonly referred to as the Common Rule. Although difficult to navigate in an era of usernames and reidentification, review boards will determine whether subjects' privacy is sufficiently protected.[209]

Predictive analysis and experimentation may be less universally valued

---

Charles A. O'Reilly, *Individuals and Information Overload in Organisations: Is More Necessarily Better?*, 23 ACAD. MGMT J. 684 (1980).

208. Paul M. Schwartz, *Data Protection Law and the Ethical Use of Analytics*, THE CENTRE FOR INFORMATION POLICY LEADERSHIP (2010), http://www.huntonfiles.com/files/webupload/CIPL_Ethical_Undperinnings_of_Analytics_Paper.pdf.

209. Patricia Cohen, *Questioning Privacy Protections in Research*, N.Y. TIMES, Oct. 23, 2011, http://www.nytimes.com/2011/10/24/arts/rules-meant-to-protect-human-research-subjects-cause-concern.html?pagewanted=all.

when compared to the value placed on that of cultural history. The story of *Flaubert's Parrot* outlines a similar dilemma to the one presented by the right to be forgotten. The protagonist is on a search for truth of the past, the life of Gustave Flaubert, an ardently private man with a protected reputation as a recluse. An acquaintance significantly underpays an unknowing woman for letters between Flaubert and a lover. The protagonist is mortified when the acquaintance explains that he destroyed the letters at the request of the author, Flaubert, who had ended the series of letters with the instruction to his lover. Here we find an unfair transaction for personal information of an individual who had explicitly stated the information was to be deleted; the historical information is at the mercy of subjective judgment. Today, are we any better equipped to address the appropriate actions of those that hold the information?

Perhaps we are. Archeology and library ethics are certainly not undisputed or easy to practice, but they are examples of use regulation related to maintaining the integrity of information and the dignity of subjects in the pursuit of knowledge. An interesting excavation practice involves leaving some of the site untouched for future researchers who may seek different answers or have improved methods of extracting more precise or enriched information from the site.[210] Similarly, archivists are guided by the Archival Code of Ethics. The Society of American Archivists has drafted a Code of Ethics that states:

> [Archivists] establish procedures and policies to protect the interests of the donors, individuals, groups, and institutions whose public and private lives and activities are recorded in their holdings. As appropriate, archivists place access restrictions on collections to ensure that privacy and confidentiality are maintained, particularly for individuals and groups who have no voice or role in collections' creation, retention, or public use.[211]

The information holding the skinny dipping college student may be important to a collection of images representing the first generation of digital natives in college, sociological research on expressions of sexuality, or predictions on future courses of action when included with other information. The rape victim content may be important to figures on the sexual violence reporting or commentary surrounding such crimes as well as the prediction and prevention of such acts. Information regarding the non-payment of child support is relevant to determining reasons for non-payment to help improve the system as well as impacts on the child over the course of his or her lifetime. The racist tweet could be very relevant to assessing social progress. Information will change in relation to immediate and remote needs over the course of its life cycle; this breakdown provides policymakers with a structure for balancing the demands of contested access to old information.

---

210. David Frankel, *The Excavator: Creator or Destroyer?*, 67 ANTIQUITY 875, 875-877 (Dec. 1993).

211. *Code of Ethics for Archivists*, SOCIETY OF AMERICAN ARCHIVISTS (2011), http://www2.archivists.org/statements/saa-core-values-statement-and-code-of-ethics.

C. *Information Life Cycles*

Having outlined two categories of information needs, the way in which information meets those demands as it ages is also outlined. Yet, the attributes of old information have not been outlined or organized outside of a small number of disciplines, and have rarely, if at all, been considered in legal scholarship. The following organizes the phases of an information life cycle in a descriptive fashion. The principles of information perishability and unpredictable value are the centerpiece for the following analysis, but other considerations are important to the assessment or measurement of information value over time. Focusing on information as a form of communication and representation helps to distinguish its use and value over time into phases.

1. *Distribution Phase*

Upon release, information holds a unique status. It is novel, contributes to the knowledge base and is heavily sought after, shared, and used. Internet memes and news are examples. Information at the distribution phase is an accurate representation of *something* in the world and held within the context it was created. At that moment the piece of information, sentence, data, figure, or image symbolizes something—an address, an opinion, a reaction, the best way to dice an onion, how many planets are in the solar system, that the world is flat. These expressions represent someone's interpretation of an aspect of the world as it stands.

The information is also a reliable communication from the speaker. At the moment of release, the speaker intends to communicate the message held in the information. The information communicated may not be valuable, but the act of communicating is valuable; the value of the freedom of expression has been well articulated.

There is also a sense of justice in the priority of speech over privacy at this point. The information subject should be accountable for her actions and interactions. The existence of the information online and the limitations it may impose on the subject will act as a deterrent to others. Exposure as a deterrent is very powerful, but as a society we have not collectively established those behaviors that should be deterred and those that should be protected even against our most salacious interests.

Immediate value is at its highest at the distribution phase. New information is the most accurate representation of the state of the world and communication from the speaker. Therefore, current information allows us to make the best decisions. For companies this information is operational and necessary to functioning efficiently. A company wants your current address to ship your order. For those wanting to hire an employee or create a relationship, the skinny dipping image may not reflect the maturity or other traits desired by the employer in an employee. The non-payment of child support may have a similar impact on decisions; someone dodging child support may not be an

ideal date or employee. An employer making a decision about an applicant may want past information, but the old information may lead to poor decisions, because it overshadows the current state of the applicant. A city determining how much funding should go to a sexual violence clinic may have an immediate need for the information that a rape has occurred and the details of the victim. The racist comments from a teenager may be used by the school system to ramp up diversity education in the school. These are immediate needs that factor into operational decisions. Acxiom may have no operational needs for the subject. Amazon needs your information to mail you the correct product, but may also need it to make recommendations to you. Recommendations are lower needs than the correct address. Remote value is low at this point. The information is readily available, its value to historical or predictive research may be difficult to ascertain, and it may need to be combined with other information that is not yet available.

2. *Record Phase*

What happens to information when it is no longer newsworthy? At the record phase, information becomes stale and subsequently may need verification and is not sought out by the general public. For instance, GoogleTrends shows that interest in Alexandra Wallace only existed for a few weeks in 2011. This information has been absorbed into the knowledge base and its finer details may no longer be passed on.

Records are often reduced for manageability and efficiency. Information, as a representation of something, generally becomes less accurate over time. The "something" that it represents may have changed, but the piece of information stays the same, and so it requires effort to verify its accuracy. Wikipedia can be quite a bit more useful than an encyclopedia because it can be updated with current information.

Information also becomes less reliable as a communication from the speaker. Few of us continue to talk about the same thing over time or talk about it in the same way. We may no longer feel the need to communicate information found on our blogs or other formats, but the information remains. Many of us stop caring about the things we cared about a few years ago or see things differently as we learn and experience more. If our communications are not managed, those thoughts can cause problems for both the communicator and the subject of the communication. How many users delete blogs, pictures, or other content without considering whether valuable information may be destroyed? How many users go through old content to update or edit it? How many users consider whether the information may have very low value but significant harms?

Information loses context over time. It becomes displaced from its original setting. For instance, pictures stored on personal computers without tags, dates, or files may be discarded because they do not contribute to a story or sentimental moment. Information without context not only decreases in value

but can be frustrating and dangerous. It is common to experience moments of judgment or assessment by another who was missing the whole story – they did not hear the whole story. Print publications solely reporting on those arrested in a local area have spawned free websites that include mug shots, names, and charges that are fully indexed by search engines. These arrests may lead to convictions or acquittals or may be a simple case of mistaken identity—the rest of the story is not told. Context offers a much more informed citizenry, but is not a consistent part of the Web.

Immediate and remote needs for information at the record phase are difficult to assess. Verification of continued accuracy or other resources may be necessary to record information in order to make the best decisions for immediate information needs. It may be difficult to determine whether the information is relevant, contextualized, accurate, or should be used in decision-making. When was that skinny dipping picture taken and under what circumstances? Did the father ever make or try to make any payments? Were the racist tweets made in response to some other conversation? How has the rape victim coped with the crime? Has a user dramatically changed interests since the last time data was collected? These questions put speed bumps in the decision making process. For remote needs, capturing the information while situated in its original context may become problematic at the record stage and it may not be clear that the information should be captured or processed.

3. *Expiration Phase*

Expiration occurs when the substance of the content changes but the information stays the same or the communication is no longer being actively expressed – the world or speaker has moved on, but the data record is stuck in time. The encyclopedia holds information that was accurate when it was printed but is no longer an accurate representation of the state of the subject. Blogs may communicate an idea from years ago that the author no longer communicates. Context, such as time markers or updates, can help maintain information in the expiration phase, but without context this information may require intervention to prevent harms and retain value.

Immediate information needs are not benefitted by incorporating information at the expiration stage. When the skinny dipper is no longer engaging in such activities, the rape victim has moved on, the dead beat dad becomes a good father, and the teenager is no longer racist, acting on old information may not meet immediate needs that would be better benefitted with current information regarding the character of the information subjects. Information will eventually no longer represent the state of the world or the communication of the speaker. For instance, information that reads "the world is flat" is no longer helpful for making decisions when the information "the world is round" has been disclosed. A company is not benefitted by your old address if it is trying to send you a package. But, your old address may be relevant for historical or predictive needs. If a company is tracking the

migration of its largest market from New York to Arizona, it may better predict the needs of an aging customer base. Remote information value is at its highest when things start to change because its existence is threatened – it is important to capture information as a representation of the past or previous communication before it has changed.

Based on the above, users of all types alter access to information through action or inaction at some point. Information may be unindexed to quarantine it from everyday engagement and still preserve its existence. It may be anonymized to limit liability or harm to identified individuals and still retain much of its value. It may be archived in a separate space specifically designed to manage old information. It may be reduced and organized to retain some context without increased resources. It may be deleted to simply get it out of the way. Nothing may be done and the information is buried or through neglect, loses its access point and dies. Or, the information may be associated with something painful and access is manipulated to limit exposure to those feelings.

This assessment of old information supports and opposes oblivion, but it also explains *why* the Web is quite ephemeral on its own. The Web is a human communication system and its content is human-created. We do not care to continually communicate the same thing as our interests move forward; information as representation loses value over time because it does not support operational decisions as well as new information. It is natural for communicated information to decay and be buried. While some people may choose to communicate the same thing over a long period of time, a new information life cycle begins for each information contribution over that continuation. We are left with those that value the information as something that was communicated or that represented some aspect of the past. These values are generally handled through the regulation of use or access, as opposed to deletion.

IV. A PARTIAL DEFENSE OF THE EU RIGHT TO BE FORGOTTEN LANGUAGE

Although information may retain value over the course of its life cycle, it does not retain the same type of value. Information may not be valuable for immediate needs toward the end of its lifetime, but once information has exhausted its operational purposes, it may still retain value to historical social scientists and predictive analysts. Generally, there is no way for researchers to know what information will be relevant, useful, or valuable until time has passed. Information freely available at a continuum, meaning throughout its life cycle, is dangerous to both the recipient and subject of the information. The option to intervene is necessary for both privacy (personal information may linger and cause harm long after is appropriate) and preservation (socially valuable information may become inaccessible over time). The proposed language in the EU Regulation acknowledges that personal information may need to be retained for remote needs but grants the user an amount of power that disrupts the information life cycle by ignoring the important element of

time. By more fully incorporating the way in which information ages, the right to be forgotten can protect the privacy rights of the subject with little social impact.

A. *On the Right Track*

Revisiting the language proposed by the draft of the E.U. Regulation, vagueness leads to interpretations that are both severe and toothless. As stated above, Rosen has pointed out that the language would allow a user to remove content about her posted by another on a site with which the user had no dealings.[212] But, the language could just as easily be read to mean that a data controller may always claim to retain user data for statistical or historical reasons.

> [D]ata subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.[213]

The exceptions read:

> However, the further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.[214]

Based on the needs of information users over time and the way in which information can meet those needs as it ages, this language is close to maintaining the immediate and remote needs of information users while protecting privacy. If personal information is not as valuable as it ages through distribution to record to expiration phases – because it is accessed less, discounted as possibly inaccurate of the current state of the individual, increasingly uncontextualized, and, depending on the social violation, a privacy invasion—limiting access to the information would have few negative implications. The proposed E.U. Regulation language reflects how aging information becomes less valuable to general public information users, but may retain high value for researchers and historians. The way in which this language is finalized and interpreted will determine the future of this movement, but further guidance for data controllers is vital.

The information life cycle perspective outlined above supports a right to be forgotten that allows harmful personal information to become less accessible as

---

212. Rosen, *supra* note 95.

213. *Proposed Data Protection Regulation*, *supra* note 90, art. 17(1)(a)-(d), at 51.

214. *Id*. art. 17(3)(a)-(d), at 52.

it meets fewer information needs, and also helps sort out some of the inevitable issues that arise from granting such a right. There are difficult and obvious concerns raised by how the right to be forgotten could and should function, some mentioned in Part I(C). The following is a discussion of how the life cycles perspective responds to these concerns and how the perspective can be further integrated into proposed legislative language. Section D of this Part argues that the language needs to incorporate an element of time in order to protect the interests of information users in an effort to protect the privacy of the subject.

B. *Revived Interest*

The difficult task inherent in information preservation is determining what information may have future value. All six of our scenarios involve information whose immediate value may decay as remote value ripens. When immediate needs are no longer being met it may be "fair" to disassociate the individual with the information, which may also protect the decision-maker from making poor decisions. While a complete history of an individual may lead to unfair and poor decisions, there are certain roles where the public has traditionally been entitled to a complete history, such as political office. Voting is an immediate need that correctly or incorrectly relies on old information. Most people do not run for political office, a role that is particularly exposed by special information practices and standards,[215] but any four of the individuals from the scenarios could run for office. Deleting associations between individuals and their past is dangerous, but maintaining the association with access and use restrictions may prevent the disappearance of personal pasts with the ability to re-establish full access and use upon the presentation of a new immediate need, such as voting.

In a few years, Alexandra Wallace may still be making racist videos or she may be running for political office. These facts help to determine the value of her name being associated with a piece of negative information. Preserved information may still be very accurate (if she is still creating racist media) or relevant (if she is running for office)—it could retain or regain much of its value. More likely, she will try to disassociate herself with the content as best she can[216] so she can pursue a normal job and maintain normal relationships. When she is searched, she will be at the mercy of the employer or prospective friend. Wallace is hardly the most sympathetic of online reputation victims and

---

215. The public figure doctrine announced by the Supreme Court in *Curtis Publishing v. Butts*, 388 U.S. 130, 173 (1967), held that a prominent public person had to prove actual malice, knowledge of falsity or reckless disregard of whether a statement is true or false.

216. Wallace has already removed videos using DMCA takedown notices. *Student in Asian tirade video quits university after 'death threats and harassment,'* DAILY MAIL (Mar. 19, 2011), http://www.dailymail.co.uk/news/article-1367923/Alexandra-Wallace-YouTube-video-Student-Asian-race-row-quits-Californian-university.html.

her video sparked a large amount of interesting debate. Questions for the right-to-be-forgotten debate, however, should be: whether her name adds to the value of the content; whether the information remains accurate; and whether the information does more harm than good after a period of time. Determining whether information will have future value is an exercise that is much more calculated and insightful at the expiration phase than the distribution phase. More time means more perspective on access decisions.

Rehashing the past is an excellent subject for distinguishing the life cycle approach. Under Swiss law, for example, the media is not entitled to identify an individual with his criminal past after sentencing has occurred–it is no longer newsworthy.[217] Countries with this type of formalized expiration phase have determined that immediate information needs are not or should not be supported by old information. The social and individual value of rehabilitation outweighs the public's right to the name of the individual involved in the prior criminal conduct. "The truth of the facts could no longer justify the infringement of the plaintiff's right to have his honor and his private life respected."[218] The Second Circuit Court of Appeals ironically protected the publication of information legally available even when it rehashes the past.[219] In *Sidis v. F-R Publishing Corp.*, the details of a child prodigy's adult reclusive life were protected as "newsworthy" over the privacy rights of the information subject.[220] Similar to *Sidis*, the information life cycle approach would conflict with the European form of forgetting because the single piece of information would be assessed similar to a file. Old information that is newly distributed gains a new life cycle – a new file is created. Information is assessed upon its point of distribution, not the original point in time when the substance of the information occurred, and a willingness to continue to re-distribute suggests high value.

The '95 E.U. Directive addressed the differences between information throughout its life cycle, albeit briefly, vaguely, and somewhat indirectly. Art. 6(1)(e), directs personal data to be kept in such a way that identifying data subjects is permitted for no longer than necessary for the purposes of which the data was collected or further processed, and safeguards should be put in place for stored personal data held longer for historical, statistical, or scientific use.[221] Art. 12(b) guarantees that a data subject may rectify, erase, or block the processing of data if it is incomplete or inaccurate.[222] The proposed E.U. Regulation includes a similar exception in art. 17(3) for the retention of data

---

217. Werro, *supra* note 78, at 285.

218. *Id*. at 290.

219. *Sidis v. F-R Publishing Corp*., 113 F.2d 806 (2d Cir. 1940), cert, denied 311 U.S. 711 (1940).

220. *Id.*

221. Council Directive 95/46, art. 6(1)(e), 1995 O.J. (L 281).

222. *Id*., at art. 12(b).

where it is "necessary for historical, statistical and scientific research purposes, for reasons of public interest in the area of public health, for exercising the right of freedom of expression, when required by law or where there is a reason to restrict the processing of the data instead of erasing them."[223]

Without more guidance, the E.U. Regulation will not quell fears about rewriting history. It alludes to an information life cycle, but in reality may not protect against unwanted deletion. Assume a data subject contacts a data controller that has made her information public to erase the content. The data controller may be able to keep it for historical purposes, but may erase it because it is simply easier and less dangerous. Preservation efforts are already insufficient. Limiting access and use restrictions as opposed to deletion are better forms of protecting information in the expiration phase for future information needs. Finally, for only $29.95 anyone can have a mug shot entry removed from LookWhoGotBusted.com.[224] Sites like Reputation.com[225] make the "integrity"[226] of history or the "objectivity"[227] of the Internet, at least as it relates to individual history, questionable, because they allow users to rewrite our history for a price.

C. *Personal Searches vs. Public Interest*

When an employer searches a possible candidate, a parent searches a child away at college, a new acquaintance searches for a bio, or a targeted marketing technology seeks to provide enticing ads to a user, the searcher is probably interested in everything, but that does not mean they have a right to or legitimate interest in discovering all of the personal information attached to an individual. A personal search or the processing of personal information does not necessarily serve the public interest. For instance, below are the Google Trends results for Caitlin Davis, the 18-year-old New England Patriots cheerleader who was fired after pictures were posted online showing her posing next to a passed-out friend who was covered in sharpie markings including a swastika,[228] and Alexandra Wallace, the UCLA undergraduate student that

---

223. *Proposed Data Protection Regulation*, *supra* note 90, art. 17(3)(a)-(d), at 52.

224. LOOKWHOGOTBUSTED: YOUR SITE FOR CONSTANTLY UPDATED MUGSHOTS, http://www.lookwhogotbusted.com/custom-mugshot-removal-service?r=762666# (last visited Jan. 30, 2013).

225. The site, Reputation.com states "Misleading, inaccurate or negative links in your search results adversely affect the impression you make when people 'Google' you and can materially impact you or your business," and that "since it's nearly impossible to get posts deleted, our patented technology makes damaging content nearly impossible for anyone to find." REPUTATION.COM, http://www.reputation.com/myreputation (last visited Jan. 30, 2013).

226. Granick, *supra* note 105.

227. Hendel, *supra* note 3.

228. Gayle Fee & Laura Raposa, *Caitlin Davis' life is not so cheery now*, THE BOSTON HERALD, Nov. 5, 2008, http://bostonherald.com/track/inside_track/view/2008

posted a racist rant about her Asian colleagues on YouTube that quickly went viral.[229]

FIGURE 3. GOOGLE.COM/TRENDS SEARCH RESULTS FOR "CAITLIN DAVIS."

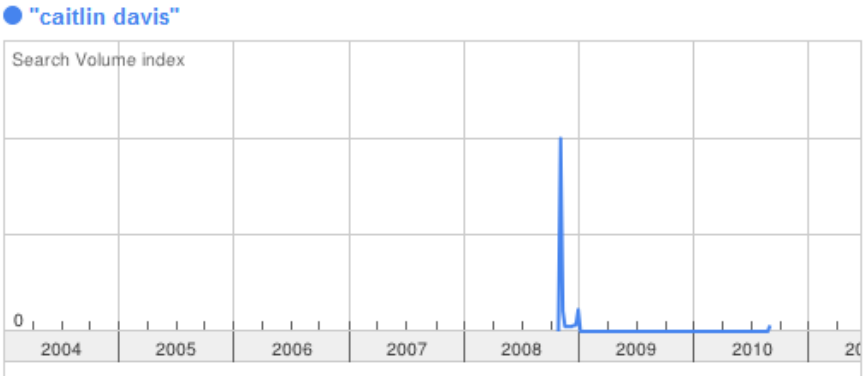
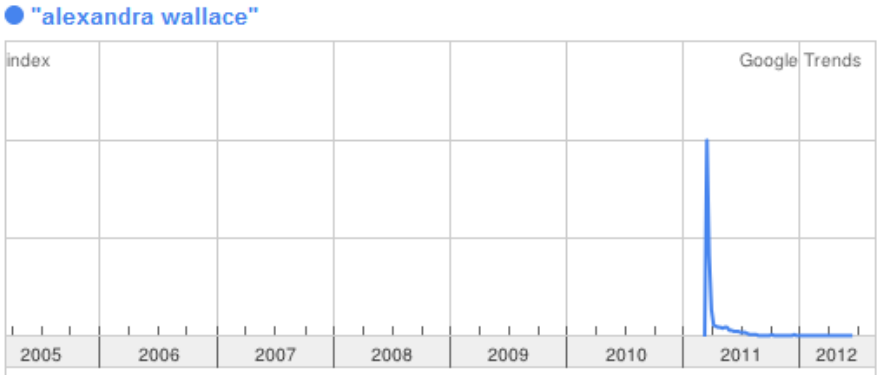


FIGURE 4. GOOGLE.COM/TRENDS SEARCH RESULTS FOR "ALEXANDRA WALLACE."



These are two of the least sympathetic, and perhaps least likely indiscretions to be forgotten. There are also individuals that are much more innocent, whose stories have somehow caught the attention of a well-read blog, site, or Twitter feed. Much more common are the many individuals that may want to move beyond personal information that has never been "trending," and may never get more than a few hits that dwindle in number over the years.

_11_05_Caitlin_Davis_booted_from_Patriots__cheering_squad.

229. *Alexandra Wallace, Student in Anti-Asian Rant, Says She'll Leave UCLA*, THE HUFFINGTON POST (Mar. 19, 2011), http://www.huffingtonpost.com/2011/03/19/alexandra-wallace-student_n_837925.html.

Wikipedia's Biographies of Living Persons Policy draws a distinction between general public interest in the individual or the event or topic of an entry. It reads:

> Caution should be applied when identifying individuals who are discussed primarily in terms of a single event. When the name of a private individual has not been widely disseminated or has been intentionally concealed, such as in certain court cases or occupations, it is often preferable to omit it, especially when doing so does not result in a significant loss of context. . . Consider whether the inclusion of names of private living individuals who are not directly involved in an article's topic adds significant value.[230]

Based on this policy, the Star Wars Kid is not named in the entry on the Star Wars Kid.[231] Similarly, Wikipedia has a deletion policy that results in five thousand pages being deleted each day, one reasoning being a lack of "notability," which requires significant coverage, reliability, sources, independence from the subject, and a presumption that the subject is suitable for inclusion.[232] Articles with unclear notability should not resort to deletion, but those that are clearly not notable should be deleted and useful material preserved on the talk pages,[233] which are not indexed by Google.[234]

Like Wikipedia, the right to be forgotten could (but does not) ask the difference between public interest and private searches in order to determine the right course of action when a user seeks to have personal information "forgotten," as opposed to quick deletion or automatic First Amendment preservation. This is similar to assessing the information needs over time. An individual may be a public fixation for a time, but not relevant to the story that once captured the public interest, collected for historical purposes. Compare the GoogleTrends search results for "ghyslain raza" and "star wars kid" below.

---

230. *Wikipedia: Biographies of living persons*, WIKIPEDIA, http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy (last modified Feb. 3 2013 at 19:11).

231. *Talk: Star Wars Kid*, WIKIPEDIA, http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid (last modified Jan. 9 2013 at 02:49).

232. *Wikipedia: Notability*, WIKIPEDIA, http://en.wikipedia.org/wiki/Wikipedia:Notability (last modified Jan. 16 2013 at 17:31).

233. *Id*.

234. *Wikipedia Talk: Talk Pages not Indexed by Google*, WIKIPEDIA, http://en.wikipedia.org/wiki/Wikipedia_talk:Talk_pages_not_indexed_by_Google (last modified Jun. 27 2013 at 05:33).

FIGURE 5. GOOGLE.COM/TRENDS SEARCH RESULTS FOR "GHYSLAIN RAZA."

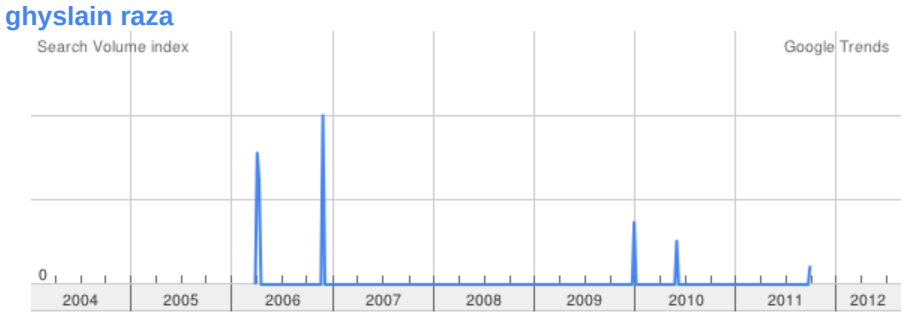
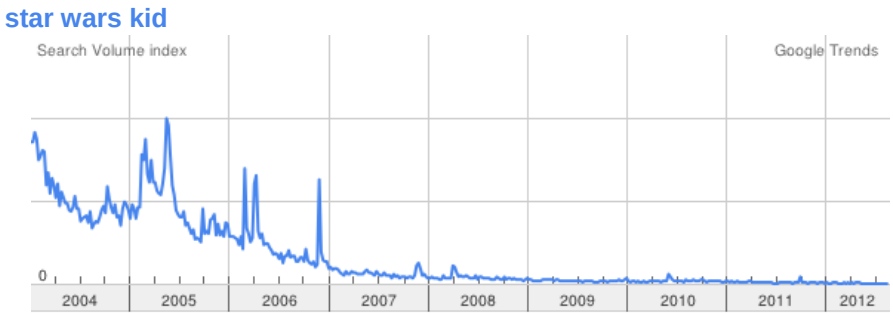


FIGURE 6. GOOGLE.COM/TRENDS SEARCH RESULTS FOR "STAR WARS KID."



When the German Federal Court of Justice heard the first lawsuits initiated by Lauber and Werlé, it was to determine whether the storage of old news stories in online archives was the equivalent to a current dissemination of the story; in other words, is providing continual access to online content essentially the same as publishing a new story?[235] Disseminating information that associates an individual with his criminal past may violate the personality rights of those reintegrating into society after serving a criminal system depending on how much time has passed since the offense, the harm to the offender, and whether new coverage has been triggered by some act of the offender.[236] In deciding cases of archived internet content, the German Federal Court of Justice devised a two-part test to settle inconsistencies among lower courts. Some find the online archive the same as a current, and therefore new, dissemination of the story and others find the online archive comparable to traditional archives.[237] The Court of Justice asked both how the report was

235. *See* Bundesgerichtshof [BGH] [Federal Court of Justice], No. VI ZR 217/08 (Dec. 15, 2009) (rainbow.at); BGH, No. VI ZR 227/08 & 228/08 (Dec. 15, 2009) (Deutschlandradio); BGH, No. VI ZR 243/08 & 244/08 (Feb. 9, 2010) (Spiegel online); BGH, No. VI ZR 245/08 & 246/08 (Apr. 20, 2010) (morgenweb.de).

236. *Id.*

237. *Id.*

disseminated and how the reader will perceive it.[238] Dissemination of information that is deemed minor, such a listing in a website calendar or teasers that lead to pay-to-view archives, will not violate personality rights.[239] The court compared actively searching for the specific information online to prime time television coverage.[240] If the content must be actively searched, as the Lauber and Werlé content was, the publication is not a violation, but if it is pushed onto the reader or brought to the attention of a reader through links from current content, the publication might constitute a violation.[241] The second part of the test requires that the archived information not give the impression that the content is current or a fresh publication.[242]

The two-part test determines whether online archives are a new or current publication, which is not precisely the issue raised by the digital right to be forgotten. But this type of interpretation of personality rights has traditionally granted a right to be forgotten, and therefore, the Court's analysis is relevant. Neither the traditional nor the new German interpretation of the right to have one's criminal past forgotten align with the life cycles approach. This is because the fresh dissemination of content resets the information life cycle. The creation of new content about a criminal past holds high value to the communicator and potential users in the distribution phase and would not be restricted under a life cycle analysis. However, once the content is born online, its life cycle begins and its harm to the subject can be assessed against other information needs. The analysis of the German Federal Court of Justice does not address the value of the information; the Court determines that if a user must actively search for the content, it does not violate the personality rights of the plaintiff. This aspect of the decision does not address current information behavior; active online searching is a gateway to all media today, including television documentaries. What online information is actually pushed on a user? Almost all content is actively obtained. The second prong of the test requires that a reader will perceive the information as dated. This certainly falls in line with a life cycle approach, because it presents an accurate time to the user and any technical system inclined to recognize the date. The life cycle approach seeks to enhance the overall value of content on the Web by measuring the interest of the communicator, immediate, and remote users in light of the harm to the individual.

A similar case came to the New York Court of Appeals, the state's highest court, in *Firth v. New York*, 98 N.Y.2d 365, 368-69 (2002). A New York state employee attempted to bring a defamation claim for a report criticizing him on a state agency's website, but the report had been posted online for more than a

238. *Id*.
239. *Id*.
240. *Id*.
241. *Id*.
242. *Id*.

year; the statute of limitation had run on the claim.[243] Firth argued that because the page had changed within the year it constituted a republication.[244] Because the page could be altered at any time, Firth argued that the defamation statute of limitation "should not be applied verbatim to defamatory publications posted on the Internet in light of significant differences between Internet publications and traditional mass media."[245] The court disagreed, choosing to treat online archives the same as traditional print archives.[246]

The single publication rule emphasized by *Firth* also violates a life cycle approach because it only looks at a piece of information once, in the distribution phase. False information has very low value and significant harms. Easy access to false information for immediate and remote information users is harmful to all parties. The purpose of the right to be forgotten is to deal with true personal information and may be difficult to categorize as a defamation type of right or claim. Still, the harms to the subject as well as immediate and remote users created by false information is not justified under a life cycle approach. Particularly with a medium that may be so corrected – maintaining accuracy, context, and utility are the priority of the approach.

D. *A Lack of Time*

While the E.U. right to be forgotten language somewhat embraces the lifecycle of information, it is missing an important element: time. Currently, harmful personal information can linger as its value decays and perhaps even becomes misinformation. The current language of the draft E.U. Regulation would grant data subjects much more control over personal information that has been collected. Information asymmetry between user and data controller has driven some scholars to argue the right to be forgotten must be a right to delete in order to shift power back into the hands of users. Allowing users to withdraw consent or object to processing their information does not recognize the many interests in information, the life cycle of information, and may be an overcorrection of the current imbalance. The user may want to restrict access to or delete personal information while it is still of public interest or something more than strictly an individualized personal search – it may still have a great deal of immediate need value to a large number of searchers with a wide range of interest in its personalized form.

The Do Not Track Kids Act's eraser button similarly lacks the important element that allows information to age through the life cycle, and in turn, protect its availability for other information needs. Included in the findings of the bill, 94% of adults and parents believe that individuals should have the

243. Firth v. New York, 98 N.Y.2d 365, 368-69 (2002).
244. *Id*. at 369.
245. *Id*.
246. *Id*. at 370.

ability to request the deletion of personal information stored by a search engine, social networking site, or marketing company *after a specific period of time*.[247] However, this belief is not represented in the language of the statute, which permits, to the extent technologically feasible, users to erase or otherwise eliminate content that is publicly available through the site that contains or displays personal information of children or minors.[248] The only exception is for compliance other Federal or State laws.[249] Without an element of time there is no element of accountability. Time is an important aspect to the analog right to be forgotten in Europe; it balances the right with the interest of other information users.

A user should be able to express objections to the continued processing of personal data in a way that is recognized by the data controller. However, that request must be weighed against the needs of the information to the data controller, as well as immediate and remote uses. The statutory language of a right to be forgotten could include an arbitrary time that adheres to both data retention laws, meaning that after data has been stored for the required time it may be anonymized, deleted, or access limited if a user has invoked her right to be forgotten and it has been a designated number of years. Although more difficult to draft and program, language that would allow for the right to be executed after the information has entered the record or expiration phase would better meet the many information demands than an arbitrary time frame. Information that has been published (publicly accessible online) may encourage different action by or options for the data controller, e.g., limiting access or use as opposed to deletion. These specifics are beyond the scope of this article, but should be considered with the information life cycle in mind. The addition of time as a statutory element supports balance between user control and the information needs of others.

The impact of time on information value and privacy interest was specifically articulated by the US Supreme Court in *U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press,* 489 U.S. 749 (1989). The Court outlined a concept of "practical obscurity" for interpreting FOIA disclosures that fell under the privacy protections in Exemptions 6 and 7(C).[250] The "practical obscurity" concept "expressly recognizes that the passage of time may actually increase the privacy interest at stake when disclosure would revive information that was once public knowledge but has long since faded from memory,"[251] The Court adds, "[o]ur cases have also recognized the

247. Do Not Track Kids Act, *supra* note 99, § 2(17), at 5.

248. *Id.* § 7(b)(1)(A), at 24.

249. *Id.* § 7(b)(2).

250. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 767 (1989).

251. *Exemption 7c,* Department of Justice Guide to the Freedom of Information Act 2009, 579, *available at* http://www.justice.gov/oip/foia_guide09/exemption7c.pdf (*citing* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 767

privacy interest inherent in the nondisclosure of certain information even when the information may at one time have been public."[252] Put slightly differently in *Rose v. Dep't of the Air Force*, 495 F. 2d 261, 267 (2d Cir. 1974), "a person's privacy may be as effectively infringed by reviving dormant memories as by imparting new information."[253]

In a case related to the maintenance of information under the Privacy Act, the DC Court of Appeals was to determine only the retention of records, not its initial collection or disclosure.[254] Lindblom, president of the MacArthur Foundation, became aware of interest from the FBI and pursuant to the Freedom of Information Act, 5 U.S.C § 552(a), requested copies of all documents relating to him.[255] A number of redacted documents were disclosed while others were not released under exceptions 1, 2, 7(C), and 7(D).[256] A number of challenges to the limited disclosure were made, but most notable is the argument that § (e)(7) of the Privacy Act, which forbids a government agency from maintaining records on an individual's first amendment activities unless pertinent to and within the scope of authorized law enforcement activity.[257] Lindblom argued that, "information which may have been properly collected as part of a legitimate law enforcement investigation may not be permanently kept under the name of the individual, especially when that individual is not the target of the investigation."[258] The court, however, found that "authorized law enforcement activity" does not mean the record "must be pertinent to an active investigation." Information, once expunged, is "gone forever," and "[i]nformation that was pertinent to an authorized law enforcement activity when collected does not later lose its pertinence to that activity simply because the information is not of current interest (let alone 'necessity') to the agency."[259] Although the immediate use of the information may pass, it is preserved for remote uses. Time here does not impact the retention of the record. As demonstrated in *Reporters*, the information's access, use, and disclosure may be limited.[260]

The importance of time should not be overlooked and should provide an important point of contention for U.S. advocates voicing concern and

---

(1989)). See also Rose v. Dep't of the Air Force, 495 F.2d 261, 267 (2d Cir. 1974).

252. *Reporters Comm.,* 489 U.S. at 767.

253. See also Assassination Archives & Research Ctr. v. Cent. Intelligence Agency, 903 F. Supp. 131, 133 (D.D.C. 1995) (finding the passage of three or four decades, "may actually increase privacy interests.").

254. J. Roderick MacArthur Found. v. Fed. Bureau of Investigation, 102 F. 3d 600 (1996).

255. *Id*. at 601.

256. *Id*.

257. *Id*. at 602.

258. *Id*.

259. *Id*. at 603.

260. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749 (1989).

compromise on the right to be forgotten in Europe, as well as at home. Accountability, balance, and better decisions related to information at issue are all benefits that flow from the addition of time into any digital right to be forgotten. Only time allows for information to reach the expiration of its life cycle, mitigate the impact of a right to be forgotten on the Web, and protect the privacy rights of its users.

CONCLUSION

"Gossip isn't inherently good or evil—it has its virtues as well as its vices. On the Internet, however, gossip is being reshaped in ways that heighten its negative effects and make its sting more painful and permanent," explains Solove in his book *The Future of Reputation*.[261] As of today, four, almost five, years later, more than a quarter of the URLs cited as references in the book have suffered from some form of linkrot, and do not take the reader to the intended content, if any content at all.[262] Perhaps this rate of decay is enough to regulate in the name of permanence, but the librarian or historian is not likely enthusiastic about that figure. The truth is that we do not know how permanent content on the Web is or what type of information lasts longer than it should, who produces it, or how it is maintained. The dead links in Solove's citations range from government documents to content produced by well-established magazines to personal blog bio pages.

"Who controls the past controls the future,"[263] an often quoted line from *1984*. History found online is threatened by its fleeting digital and human communication. Digital information does not naturally last forever, nor does it last long in anthropological terms. Looking back on all the formats used to preserve information that would later become important historical anecdotes or markers, those built in binary, interpreted by constantly updated code, maintained by decentralized users, and organized by institutions able to preserve a tiny portion of the Web are not the most reliable. "Right or wrong, the Internet is a cruel historian."[264] But, content persistence in fact proves that the Internet is a lazy historian with no principled practices of preserving or protecting knowledge. If online information is not more thoughtfully maintained as a collection, neither goals of privacy nor preservation will be met in the future.

There are serious consequences to the information ethics and policy

---

261. Solove, *supra* note 6, at 4.

262. The notes for the Future of Reputation with hyperlinked URLs can be found here: http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text/futureofreputation-notes.pdf (last visited Feb. 2012).

263. GEORGE ORWELL, 1984 248 (1949).

264. Solove, *supra* note 6, at 11 (citing a comment to a blog post about the Korean responses to "Dog Poop Girl," a girl who refused to pick up after her dog in a subway car which resulted in an online shaming campaign).

choices upon us. Balancing the information needs of users must be done thoughtfully and without relying on arbitrary, dichotomous distinctions between public and private information. For example, anonymization, a method of providing privacy relied upon by most privacy regulations,[265] is a tempting tool because when used appropriately it can provide privacy while keeping the value of the content intact. But, consider the Pilate Stone. A stone found in Caesarea-on-the-Sea, Israel, in 1961, it is the only archaeological find mentioning the name Pontius Pilate. The removal of names from records should not be done lightly. Each online record should be considered as a contribution to the space. Recognizing that the medium used in the Internet Age is in many ways fragile, we must consider how best to avoid a "lost era" of American history while maintaining privacy interests that promote information sharing. In order to make the best decisions for problematic information conditions, each piece of information should be assessed based on the above information with the phase of the information life cycle.

Arguments that we will sacrifice limited advances in knowledge for privacy or that the First Amendment has no room for such exceptions are not as strong as proponents would like, but neither are the threats of permanence. Because a defined privacy perspective, social goal for the Internet, and understanding of content persistence are still only developing in the U.S., deletion may be ill-advised. The right to be forgotten addresses an interesting aspect of the Information Age—accessibility to old information. Ignoring time would be a critical mistake in an effort to alleviate the harms caused by this access.

---

265. A method that has been proven quite fallible. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010).