Meg Leta Ambrose:

You Are What Google Says You Are: The Right to be Forgotten and Information Stewardship

Abstract:

The right to be forgotten is a proposed legal response to the potential harms caused by easy digital access to information from one's past, including those to moral autonomy. While the future of these proposed laws is unclear, they attempt to respond to the new problem of increased ease of access to old personal information. These laws may flounder in the face of other rights and interests, but the social values related to moral autonomy they seek to preserve should be promoted in the form of widespread ethical information practices: information stewardship. Code, norms, markets, and laws are analyzed as possible mechanisms for fostering information stewardship. All these mechanisms can support a new user role, one of librarian - curator of digital culture, protector of networked knowledge, and information steward.

Agenda:

Author:

Meg Leta Ambrose:

- ATLAS Institute, University of Colorado, Boulder, 1125 18th St., 80309-0320 Boulder, Colorado
- ☎ + 1 - 303-735-4577, megleta@gmail.com, www.megleta.com

ISSN 1614-1687

1 Introduction

We size each other (and ourselves) up through online search engines. Universities, employers, and potential romantic partners search users to discover what has not been included in the initial disclosure. Perhaps this new information practice is why 94% of parents and 94% adults feel that after a period of time, an individual should have the ability to have personal information held by search engines, social networking sites, or marketing companies deleted.[1] It is difficult to change when one cannot move beyond the past. The Internet changes access to the past and this new form of access may limit the growth and development of the individual. Facebook Timeline feels like a privacy invasion to many because old information about us has not been recalled with ease or great detail in the past. This paper details these issues and examines proposed responses to threats to moral autonomy posed by personal information accessible online. After briefly introducing the right to be forgotten, I discuss research on information persistence to properly frame the problem. I then propose wide-spread information stewardship to support responsible retention of information to prevent stagnation of the self in the Internet Age.

2 Information Landscape and Moral Autonomy

In an age when "[y]ou are what Google says you are,"[2] expecting parents search prospective names to help their kids retrieve top search results in the future, and only a few rare parents want their children to be "lost in a virtual crowd,"[3] 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."[4] Changes in the storage, disclosure, and retrieval of information have spurred governmental initiatives to prevent injustices that may arise from black marks on that "permanent record," the right to be forgotten being the most prominent.

2.1 Moral Ethics and Fluidity of the Self

Shaping and maintaining one's identity is "a fundamental interest in being recognized as a self-presenting creature."[5] The person is a dynamic pursuit of moral improvement and "cannot be identified… as something limited, definite, and unchanging."[6] When information about an individual is available in a way that she did not intend, this pursuit is disrupted. "The conception of the person as being morally autonomous, as being the author and experimentator of his or her own moral career, provides a justification for constraining others in their attempts to engineer and directly or indirectly shape the subject's identity."[7]

2.2 The Right to be Forgotten and the "Eraser Button"

The right to be forgotten is a legal response to threats to the dynamic self from modern information technology and practices. The European Commission for Justice, Fundamental Rights and Citizenship, Viviane Reding, has declared the right a pillar of the new Data Protection Directive, currently being redrafted. Although conceived as a right, value, interest, virtue, and ethical principle, I will refer to the prevention of self-stagnation by limiting access to or deleting information that has aged a certain term as a right. The roots of

[1] Zogby International Poll, http://www.ftc.gov/os/comments/privacyreportframework/00457-57996.pdf (2010).

[2] "You Are What Google Says You Are," Wired. Feb. 11, 2009.

[3] Allen Salkin, "What's in a Name? Ask Google," The New York Times, Nov. 25, 2011.

[4] *Id.*

[5] J.D. Velleman, *The Genesis of Shame*, 30 Philosophy and Public Affairs 27-52 (2001).

[6] Jeroen van den Hoven, *Information Technology, Privacy, and the Protection of Personal Data*, in Information Technology and Moral Philosophy 319 (2008).

[7] *Id.*, at 317.

the right to be forgotten are found in the prohibition of media disclosure of information related to criminal activity after the defendant has been sentenced. Being forgotten (the right to have third parties forget your past) and forgetting (the right to avoid being confronted with your past) are both embraced by the French concept *oubli*, oblivion, which 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. While a draft of the European Union Data Privacy Directive has been released, the contours of the right to be forgotten have not yet been defined. In the meantime, Google has challenged the Spanish Data Protection Agency order to remove URLs from its index that point to personal information the Agency has determined should be forgotten. A similar proposal has been made in the "Do Not Track Kids" legislation, an amendment to the Child's Online Privacy Protection Act.[8] The bill includes an "eraser button" to eliminate the publicly available personal information of children.[9]

2.3 Content Persistence

Contrary to popular notions, Web content is quite ephemeral. Information online is not permanent for a number of reasons including 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.[10] Information also loses value over time because it may become an inaccurate representation of the present, de-contextualized, and/or irrelevant.[11] Recent work suggests, albeit tentatively, that data is becoming *less* persistent over time; for example, Gomes and Silva studied the persistence of content between 2006 and 2007 and discovered a rate of only 55% alive after 1 day, 41% after a week, 23% after 100 days, and 15% after a year.[12]

If access is to be manipulated in order to protect moral autonomy, the landscape must be accurately portrayed. Information that remains online may become an inaccurate reflection of the individual as he or she changes the access to which may result in significant limitations and loss of opportunities. Information is not permanent no matter the medium, and digital mediums have their own weaknesses. Thus, without principled information practices, valuable information may easily disappear while harmful, low value information may remain longer than socially deemed appropriate.

3 Information Stewardship

3.1 Maternalistic Privacy

People once asked other people for answers. Now we ask machines, but these machines are human-created to meet human goals. At the Time & Bits conference in 1998, the attendees asked "Who is responsible?" "There are serious questions as to who will take responsibility for making digital information persist over time."[13] I propose that users take responsibility of this space as stewards of knowledge produced, used, collected, and organized online. Information stewardship is a responsibility imparted on database managers for the information they are entrusted with. Extending this ethic is a maternal, as opposed to paternal, form of privacy protection. It does not proscribe specific behaviour that is best for users or prohibit any specific

[8] H.R. 1895: Do Not Track Kids Act of 2011.

[9] H.R. 1895, Sec. 7 (2011).

[10] Henry M. Gladney, *Preserving Digital Information,* 10 (2007).

[11] R. Glazer, *Measuring the Value of Information: The Information-Intensive Organization*, 32(1) IBM Systems Journal 99, 101 (1993).

[12] Daniel Gomes and Mario J. Silvia, Modeling Information Persistence on the Web, Proceedings of the 6th International Conference on Web Engineering 1 (2006).

[13] Margaret MacLean, Ben Davis, Getty Conservation Institute, Time & Bits: Managing Digital Continuity, 19 (1998).

behaviour, but encourages users to nurture the space for long-term benefits and emphasizes the Web as a whole and as part of our social existence.

Data managers have long been stewards of the information they have been entrusted and responsible to maintain the timeliness, accuracy, and access control of the data.[14] These information stewards manage data over its lifecycle by accounting for the changing value of information from conception to disposition.[15] These basic principles underscore widespread information stewardship, which can be addressed and promoted through a number of mechanisms including markets, norms, code, and laws.[16] These mechanisms may simply allow for personal information to be less accessible over time or actively practice limiting access to or editing personal information in an attempt to minimize harm while retaining valuable substance.

3.2 Markets

The market has answered the call for reputation tarnish. Companies like Reputation.com, TrueRep.com, and IntegrityDefender.com offer services to repair your reputation and hide your personal information. On the "Suppress Negative Content Online" page of Reputation.com, the site explains that "You're being judged on the Internet," "The Internet never forgets," "The truth doesn't matter," and that you are "Guilty by association."[17] These may seem dramatic, but for those that live with a nasty link on the first page of a Google search for their name, it probably feels very accurate. Reputation.com apparently, works; it claims a 99% success rate (although any bad reviews would likely be buried).

The fact that these businesses are successful suggests that there is a market of users with injured online reputations seeking redress, that the Internet has little integrity to preserve, and that drafting laws to create hurdles to access may be unnecessary. Today, only those with means can remove themselves from the record of the Internet and those less powerful can only hope for an opportunity to explain their digital dirty laundry. While it may be appealing to demonize the "privacy for a price" approach in favor of one based on privacy for all, these services provide privacy from past negative information, a very complicated task, starting at the low price of $15 per month.

This form of intervention may promote the goals of reputation rehabilitation, but it is not information stewardship. The easiest way to make negative information less accessible is to bury it under highly ranked positive information - and lots of it. Google results can be seen as context. It is what the Web has on a user and what is the most important about them. While a reputation service can add content that adds context, it is not necessarily more accurate, relevant or valuable. Additionally, this does not offer real seclusion or the feeling of being left alone, or any other privacy definition related to autonomy. If a user is interested in seclusion, paying for a service that will plaster information about them all over the Internet, does not support their goals of regaining a private existence. If a user seeks to control information communicated about him or her, reacting to pressure to fill the Web with positive information in order to place a piece of information back in a sphere of privacy is more like strong-arming a user than empowering him or her with privacy.

The market also addresses any information a client desires. It can suppress new, old, true, false, uncontextualized, wholly fair, public or private information. In other words, these services "edit" the Internet, creating search barriers to valuable, as well as valueless, information. Relying on services that game the system reinforces the Internet as something to play with as opposed to a source of knowledge, not the goal that many have for the Internet. A real market response to information stewardship would be a movement of traffic toward up-kept content.

---

[14] Richard A. Spinello, Case Studies in Information and Computer Ethics, 7 (1997).

[15] David G. Hill, Data Protection: Governance, Risk Management, and Compliance, 57 (2009).

[16] Those set forth by Lawrence Lessig in Code (1999).

[17] "Suppress Negative Content Online: ReputationDefender: Reputation.com," https://www.reputation.com/reputationdefender.

3.3 Code

In early November, 2011, Google announced that it would be making search results "fresher and more recent."[18] The tweak affects about 35% of all searches.[19] The algorithm is now better designed to determine if a user wants to find fresh information (the score of a big game currently happening or when a concert will be coming to the area) or older information (the capital of a state or recipe for bread). How the new algorithm will impact searches for individuals is unclear, but the tailoring of search results to better account for fresh information where appropriate displays the capabilities of search engines to account for the low value of old information.

Google's main competition for the freshest information is Twitter. Twitter does not show old search results. For instance, typing in #obama2008 retrieves only 2 Tweets, both which also include the hashtag #obama2012 and were posted in the last few days. On the other hand, Twitter displays all publicly available Tweets for a user if you select their profile page. All publicly available Tweets are also collected by the Library of Congress, but are only accessible to "known researchers." These distinctions matter. Varying levels of accessibility, or the ease of retrieval, create barriers similar to those of a paper-based record society. These variations, like the old barriers, are not rooted in privacy, but information value. In order to provide the most value, information systems are managed.

4Chan, a notorious chat forum not for the faint of heart, maintains content ephemerality with thread expiration. As new threads are added, old ones get pushed down. The thread is removed permanently when it is pushed to the bottom of the fifteenth page and retrieves a "Page Not Found" error when its URL is entered. However, the thread is bumped back to the top when a user replies to the thread.[20]

These above are just a few examples of code-supported information stewardship, but the technologies need not be complex. Reminders that the information we contribute still exists and may be harmful or useful could support a more valuable online experience. For instance, after a set amount of time, a reminder would appear in email or upon sign in to a service that the user posted information identifying another individual, that the information has been crawled, and ask whether the user would like to anonymize, unindex, delete, or leave the content unchanged. Notices of information loss could also promote the preservation of possibly important information. Site owners could choose to archive the site with archive.org or another institution or allow important information to remain once long term consequences have been considered.

3.4 Norms

Shifts in norms have been offered as the solution to lingering personal information retrievable online. The idea is that we will all be used to seeing indiscretions online and will not judge people too harshly for those exposed indiscretions - after all, deep down we know no one is perfect. The opposite is also possible - norms of non-disclosure and "normalization." This section examines examples of norms related to the necessity of the identification of individuals to contribute valuable content.

The Star Wars Kid Wikipedia page does not include the name Ghyslain Raza. This is no accident;[21] Wikipedia adheres to a Biographies of Living Persons Policy which includes a presumption in favor of privacy.[22]

---

[18] "Official Google Blog: Giving Your Fresher, More Recent Search Results," Nov. 3, 2011, http://insidesearch.blogspot.com/2011/11/giving-you-fresher-more-recent-search.html.

[19] *Id.*

[20] For a more detailed study of 4Chan's content ephemerality see M.S. Bernstein, A. Monroy-Hernández, D. Harry, P. André, K. Panovich, and G. Vargas, *4chan and /b/: An analysis of anonymity and ephemerality in a large online community*, In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain (2011).

[21] "Talk: Star Wards Kid – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

[22] "Wikipedia: Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

> *"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."*

This is probably a good rule for all Internet contributions, but unfortunately, these efforts are somewhat wasted. Google search results for Ghyslain Raza return the Star Wars Kid Wikipedia as the most relevant result, highlighting the need for a more cohesive approach to old information.

The archival profession has developed and maintained a Code of Ethics to guide their practices while protecting privacy rights of donors and those that are the subjects of records. They "respect all users' right to privacy by maintaining the confidentiality of their research and protecting any personal information collected about them in accordance with the institution's security procedures."[23] Like the Internet community, the archival community is faced with a competing access principle: "Archivists strive to promote open and equitable access to their services and the records in their care without discrimination or preferential treatment, and in accordance with legal requirements, cultural sensitivities, and institutional policies."[24] With more and more archives being digitized, these decisions become more important. For instance, should diaries be digitized and accessible by anyone when they contain sensitive material about a person that is still alive? Diaries are not meant to be read by anyone but the writer and perhaps descendants, but valuable historical and cultural information has been extracted from diaries such as that of Anne Frank, Virginia Woolf, George Washington, Thomas Jefferson, William Bradford, and Sylvia Plath. The Internet Archives exclusion policy follows the guidelines set forth for traditional archives and clearly lays out the appropriate response to specific types of removal requests.[25]

Public Resource, a site that republishes court documents, evaluates and grants requests from individual's identified in the cases to remove the case retrieval by Google.[26] The documents are public records, but Public Resource will add a robots.txt file so that ethical crawlers will not index the page, and in turn, will not be presented in search engine results. The information is not deleted and still accessible through the site, but not to through a search. The above represent the norms or practices of content sources that have some sort of hierarchy and established policies, but similar ethics exist across the decentralized Internet as well. While information may be vital to capturing cultural history, identification may not. These entities protect the integrity of the information while providing a degree of privacy to the subject.

3.5 Law

When content falls through the net of the above safeguards, the law may need to step in. Some content need not rely on decay because it is inherently damaging and dangerous - toxic (e.g., social security numbers or health information). If the above means do not help the subject, perhaps legal recourse is appropriate. We must be willing to assess the value of the information, the value added by identification of the subject, and the adjustments to information we are willing to make. However, if the information supports public safety or consumer protection or identification of the subject is *still* central to the debate, access manipulation would not be appropriate.

When information is no longer newsworthy or of public interest, which can be supported by using simple tools like Google Trend and hit counts, information law is in somewhat new territory. Many victories over

---

[23] "Code of Ethics for Archivists," Society of American Archivists, SAA Council Approval/Endorsement Date: February 2005 http://www2.archivists.org/standards/code-of-ethics-for-archivists.

[24] *Id.*

[25] "The Internet Archive's Policies On Archival Integrity and Removal," drafted Dec. 13-14, 2002 http://www2.sims.berkeley.edu/research/conferences/aps/removal-policy.html.

[26] "Why is My Court Case on the Internet?" Public.Resource.Org, https://public.resource.org/court_cases.html.

the First Amendment have been won with the blow of newsworthiness, but newsworthiness is not impenetrable and has not always trumped privacy claims. Although *Sidis v. F-R Publishing Corp* is a classic case that illustrates how a broad definition of newsworthiness leaves little left of the privacy tort of intrusion and a community standard of decency.[27] The Second Circuit explained that it could not confine "the unembroildered dissemination of facts"[28] unless the facts are "so intimate and so unwarranted in view of the victim's position as to outrage the community's notion of decency."[29] The idea that newsworthiness should protect all truthful information was flatly rejected by the Ninth Circuit in *Virgil v. Time, Inc.*:

> *"To hold that privilege extend to all true statements would seem to deny the existence of 'private' facts, for if facts be facts -- that is, if they be true -- they would not (at least to the press) be private, and the press would be free to publicize them to the extent it sees fit. The extent to which areas of privacy continue to exist, then would appear to be based on rights bestowed by law but on the taste and discretion of the press. We cannot accept the result."*[30]

Both cases resulted in losing plaintiffs and unscathed defendants who were allowed to expose the private idiosyncrasies of the subjects; the facts were "simply not offensive to the degree of morbidity or sensationalism."[31]

The "zone of privacy surrounding every individual" recognized by the Supreme Court has not been carved out, but there are instances in which the court has upheld privacy in the face of expression. For example in *Melvin v. Reid*, the movie depiction of a former prostitute's real-life involvement in a murder trial impinged the successful rehabilitation of the woman and overpowered the public's interest in her past. However, since *Time, Inc. v. Hill* (1967), the First Amendment has been the predominant and determining factor in these disputes. Since then, few cases have been successful and the false light tort has dwindled to just about nothing. Deference to journalists to determine what is newsworthy and assurance that the long tail of the Internet creates an audience for everything makes for a very convoluted notion of newsworthiness as a standard for the proper dissemination of private information.

Some courts have scrutinized the individual private facts disclosed and offered plaintiffs anonymity. In *Barber* the court explained that "[w]hile plaintiff's ailment may have been a matter of some public interest because unusual, certainly the identity of the person who suffered this ailment was not."[32] The Tenth Circuit adopted a "substantial relevance" test, meaning that the individual must be substantially relevant to the published content. In *Gilbert v. Medical Econ. Co.*, the court stated that some facts are indeed beyond the sphere of legitimate public interest:

> *"Even where certain matters are clearly within the protected sphere of legitimate public interest, some private facts about an individual may lie outside that sphere... [T]o properly balance freedom of the press against the right of privacy, every private fact disclosed in an otherwise truthful, newsworthy publication must have some substantial relevance to a matter of legitimate public interest."*[33]

The newsworthiness test established by these courts reinforces the notion that just because a story is of legitimate public concern does not mean that the plaintiff's identity is necessary to disclose. A more common judicial response is reflected by the court in *Shulman v. Group W. Productions, Inc.*, which refused to make

---

[27] *Sidis v. F-R Publishing Corp.*, 113 F.2d 806, 808 (2d Cir. 1940).

[28] *Id.*

[29] *Id.*

[30] *Virgil v. Sports Illustrated*, 527 F.2d 1122, 1128 (9th Cir. 1975).

[31] *Virgil v. Sports Illustrated*, 424 F. Supp. 1286 (S.D. 1976).

[32] *Barber v. Time, Inc.*, 159 S.W.2d 291, 295 (Mo. 1942).

[33] *Gilbert v. Medical Econ. Co., 665 F. 2d 305, 307-308 (10th Cir. 1981).*

this determination regarding a woman who was identified by the news in association with a horrendous car crash.[34] The court stated:

> *"That the broadcast could have been edited to exclude some of Ruth's words and images and still excite a minimum degree of viewer interest is not determinative. Nor is the possibility that the members of this or another court, or a jury, might find a differently edited broadcast more to their taste or even more interesting. The courts do not, and constitutionally could not, sit as superior editors of the press."*[35]

The most relevant principle expressed by the Supreme Court related to privacy, access, and time came in 1989 when it decided an issue surrounding reporters' Freedom of Information Act ("FOIA") requests for criminal history records of individuals involved in organized crime and a corrupt congressman from the FBI.[36] In *DOJ v. Reporters for Freedom of the Press*, the Court outlined a concept of "practical obscurity" for interpreting FOIA disclosures that fell under the privacy protections in Exemptions 6 and 7(C).[37] 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."[38]

When confronting old information, the U.S. could attempt to draft a law that mirrors the right to be forgotten, based on the decay of newsworthiness attributed to information. There are pieces of case law that provide excellent foundations to build a privacy claim to remove or alter past information. Or the U.S. could rely on the above nudges from markets, norms, and code to support victims of the digital scarlet letter. The U.S. legal system, however, is not currently suited to force the hand of content creators or ISPs to enforce a right to alter truthful information, or its access points, distributed online. What the law can easily offer is context. In addition to the above-mentioned tools, the legal community could update an "outdated" legal claim: false light. An immense problem with negative information online is that it is often devoid of context, and therefore, misleading. Misleading information is something the U.S. legal system has experience with, albeit not much recent experience.

While false light has been called duplicative[39] and outdated,[40] thirty-one states allow the cause of action and ten have rejected it. However, in 2008 the Missouri Court of Appeals recognized that the tort may have new life in the digital age:

> *"As a result of the accessibility of the internet, the barriers to generating publicity are quickly and inexpensively surmounted. Moreover, the ethical standards regarding the acceptability of certain discourse have been diminished. Thus, as the ability to do harm grows, we believe so must the law's ability to protect the innocent."*[41]

False light claims that offer the plaintiff harmed by old information found online should be the simple addition of a timeframe. When someone suffers the financial, social, or personal harms of truthful information from their past, a false light claim would ensure that the information marked as old. Requiring at minimum a time stamp of when the content was created would allow technology to be layered on top of the added

---

[34] *Shulman v. Group W. Productions, Inc.*, 955 P. 2d 469 (Cal. 1998).

[35] *Id.*

[36] *DOJ v. Reporters for Freedom of the Press*, 489 U.S. 749 (1989).

[37] *Id.*

[38] Department of Justice Guide to the Freedom of Information Act 2009, 579 available at http://www.justice.gov/oip/foia_guide09/exemption7c.pdf, *citing DOJ v. Reporters Committee for Freedom of the Press,* 489 U.S. 749, 767 (1989) ("[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even when the information may at one time have been public.").

[39] *Jews for Jesus, Inc. v. Rapp*, 997 So. 2d 1098, 1100 (Fla. 2008).

[40] *Denver Publ'g Co. v. Bueno*, 54 P.3d 893 (Colo. 2002).

[41] *Meyekord v. Zipatoni Co.,* 276 S. W.3d 319, 325 (Mo. Ct. App. 2008).

information to promote norms for those interested. For instance, a search for an individual could be limited to content time stamped within the last 5 years. A subject should be able to demand that old information be marked as such as to not mislead potential viewers. A false light claim for identifying information that is void of the context of time promotes the goals of information stewardship and is legally, socially, and technologically feasible.

References

Barber v. Time, Inc., 159 S.W.2d 291, 295 (Mo. 1942).

M.S. Bernstein, A. Monroy-Hernández, D. Harry, P. André, K. Panovich, and G. Vargas, 4chan and /b/: An analysis of anonymity and ephemerality in a large online community, In Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media, Barcelona, Spain (2011).

"Code of Ethics for Archivists," Society of American Archivists, SAA Council Approval/Endorsement Date: February 2005 http://www2.archivists.org/standards/code-of-ethics-for-archivists.

Denver Publ'g Co. v. Bueno, 54 P.3d 893 (Colo. 2002).

Department of Justice Guide to the Freedom of Information Act (2009).

DOJ v. Reporters for Freedom of the Press, 489 U.S. 749 (1989).

Gilbert v. Medical Econ. Co., 665 F. 2d 305, 307-308 (10th Cir. 1981).

Henry M. Gladney, Preserving Digital Information (2007).

David G. Hill, Data Protection: Governance, Risk Management, and Compliance, 57 (2009).

R. Glazer, Measuring the Value of Information: The Information-Intensive Organization, 32(1) IBM Systems Journal 99, 101 (1993).

Daniel Gomes and Mario J. Silvia, Modelling Information Persistence on the Web, Proceedings of the 6th International Conference on Web Engineering 1 (2006).

Lawrence Lessig, Code (1999).

Jeroen van den Hoven, Information Technology, Privacy, and the Protection of Personal Data, in Information Technology and Moral Philosophy (2008).

Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1100 (Fla. 2008).

Internet Archive Frequently Asked Questions http://www.archive.org/about/faqs.php#29.

"The Internet Archive's Policies On Archival Integrity and Removal," drafted Dec. 13-14, 2002 http://www2.sims.berkeley.edu/research/conferences/aps/removal-policy.html.

Margaret MacLean, Ben Davis, Getty Conservation Institute, Time & Bits: Managing Digital Continuity, (1998).

Meyekord v. Zipatoni Co., 276 S. W.3d 319, 325 (Mo. Ct. App. 2008).

"Official Google Blog: Giving Your Fresher, More Recent Search Results," Nov. 3, 2011, http://insidesearch.blogspot.com/2011/11/giving-you-fresher-more-recent-search.html.

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.

Richard A. Spinello, Case Studies in Information and Computer Ethics, 7 (1997).

"Suppress Negative Content Online," ReputationDefender, https://www.reputation.com/reputationdefender.

Allen Salkin, "What's in a Name? Ask Google," The New York Times, Nov. 25, 2011.

Shulman v. Group W. Productions, Inc., 955 P. 2d 469 (Cal. 1998).

Sidis v. F-R Publishing Corp., 113 F.2d 806, 808 (2d Cir. 1940).

"Talk: Star Wards Kid – Wikipedia, the free encyclopaedia," http://en.wikipedia.org/wiki/Talk:Star_Wars_Kid.

J.D. Velleman, The Genesis of Shame, 30 Philosophy and Public Affairs 27-52 (2001).

Virgil v. Sports Illustrated, 527 F.2d 1122, 1128 (9th Cir. 1975).

Virgil v. Sports Illustrated, 424 F. Supp. 1286 (S.D. 1976).

"Wikipedia:Biographies of living persons – Wikipedia, the free encyclopedia," http://en.wikipedia.org/wiki/Wikipedia:Biographies_of_living_persons#Presumption_in_favor_of_privacy.

"Why is My Court Case on the Internet?" Public.Resource.Org, https://public.resource.org/court_cases.html.

"You Are What Google Says You Are," Wired. Feb. 11, 2009.

Zogby International Poll, http://www.ftc.gov/os/comments/privacyreportframework/00457-57996.pdf (2010).