Telecommunications Policy 38 (2014) 800–811

Contents lists available at ScienceDirect

Telecommunications Policy

URL: www.elsevier.com/locate/telpol

Speaking of forgetting: Analysis of possible non-EU responses to the right to be forgotten and speech exception

Meg Leta Ambrose

Communication, Culture & Technology, Georgetown University, 3520 Prospect St. NW, Suite 311, Washington, DC 20057, USA

ARTICLE INFO

Available online 11 July 2014

Keywords:
International privacy law
Data protection
Right to be forgotten
Expression

ABSTRACT

The right to be forgotten is contentious partly because it highlights the difference between U.S. and E.U. prioritization of information privacy and freedom of expression. Recently, a moderate amount of research has been undertaken to explore the conceptual issues underlying the right to be forgotten and how the right conflicts with the U.S. first amendment, but little has been written about its impending implementation and interoperability issues. While this is an E.U. Data Protection Regulation proposing to grant rights only to E.U. citizens, the world has a stake in this right for a number of reasons. This article will analyze the options for non-E.U. countries and data controllers, namely the U.S., to react to the establishment of such a right, now called "The Right to Erasure". These options are the following: (1) adopt the same right to erasure for themselves, (2) ignore right to erasure claims, (3) comply with erasure take down requests, or (4) seek to establish a modified version of the right to erasure. In assessing these options, the article will first address the reality of a right to erasure under U.S. law. Second, it will discuss compliance and jurisdictional issues if the right is ignored. Third, the article will look at the impact of full acceptance of the take-down regime, focusing on the potential chilling effects and abuse. Finally, it will propose that non-E.U. countries encourage a right to erasure that is less disruptive: a right to erasure that allows data subjects to directly request removal of data held privately by data controllers and a right to oblivion for publicly available information that is enforced similarly to defamation claims, requiring a court order.

1. Introduction

In 2010, the E.U. announced it would begin work to create "a new general legal framework for the protection of personal data in the European Union covering data processing operations in all sectors and policies in the European Union," and specifically noted its intent to "introduce" the right to be forgotten (European Commission, Press Release, 2010). Action taken by the data protection agency of Spain ("AEPD") against Google to force the removal of links from its index that directs users to information the agency had deemed 'forgettable' (Daley, 2011) and the language of the right to be forgotten proposed by the European Commission in its January 2012 draft of the new Data Protection Regulation ("DP Regulation, 2012") have caused a great deal of confusion and skepticism about the right to be forgotten and erasure. On October 21, 2013, the European Parliament's Committee on Civil Liberties, Justice and Home Affairs ("LIBE") adopted several amendments to the European Commission's proposal for the DP Regulation, including a title change that removes "to be forgotten" from Article 17 leaving "The Right to Erasure."

http://dx.doi.org/10.1016/j.telpol.2014.05.002
0308-5961/

While the DP Regulation is an E.U. proposal granting rights only to E.U. citizens, the world has a stake in the right to be forgotten for a number of reasons. First, content on the Internet is generally accessible around the world and the removal of content affects all users. Additionally, services that derive from big data analytics have the potential to benefit all users. Second, a great number of data controllers that will be obligated to 'erase' personal information will be outside the E.U. (Labovitz, Iekel-Johnson, McPherson, Oberheide, & Jahanian, 2010).[1] Third, designing systems to comply with one country's laws may result in 'privacy creep,' meaning systems and platforms are designed to provide deletion for users in one region, the opportunity for deletion will extend beyond that region to anywhere the platform or system is utilized.[2] Viviane Reding, the European Commissioner for Justice, Fundamental Rights and Citizenship leading the changes to the E.U. Data Protection Directive ("DP Directive, 1995"), has made it clear that "[a]ll companies that operate in the European Union must abide by our high standards of data protection and privacy," (European Commission, Press Release, 2010). Reinforcing this point in 2011, Reding stated, "Privacy standards for European citizens should apply independently of the area of the world in which their data is being processed… Any company operating in the E.U. market or any online product that is targeted at E.U. consumers must comply with E.U. rules," (European Commission, Press Release, 2011).

Of course, the eventual language of the right to erasure cannot be precisely predicted, but the article focuses on the aspects of the right that have remained consistent over the last several years as the Regulation has gone through the rule-making process. The article makes recommendations for adjustments to the right to erasure in draft form to support final language that is internationally interoperable. Compliance and enforcement expectations for those outside the E.U. are not clear (Bennett, 2012; Kohl, 2007). The article will consider ways in which non-E.U. countries, companies, and other data controllers may respond to the E.U. DP Regulation's right to be erasure as it stands in the amended version. Options for countries outside the E.U. are to (1) adopt the E.U. right to be erasure, (2) ignore the right to erasure, (3) comply with right to be forgotten take-down requests, or (4) work to establish a compromised version of the right to be forgotten that is acceptable to a number of different stakeholders. As each of the options is analyzed, the last offers the potential for the greatest interoperability, efficient cross-border functionality and preservation of national information policy values. The article concludes by proposing further medication of the right to erasure to create a version that divides its two conceptual forms (the right to delete and the right to oblivion) (Ambrose & Ausloos, 2013) and requires different procedural treatment for removal. The right to delete should only apply to passively created data trails held privately by data controllers and third parties and maintain the current E.U. DP Regulation's proposed removal notice structure of enforcement (Para.1 of Art. 17, DP Regulation, 2012). The right to oblivion should apply to information made publicly available (Para. 2 of Art. 17, DP Regulation, 2012) and require a court order, ensuring that diversity in prioritization between speech and privacy is maintained but in a manner much less disruptive to Internet communication.

2. Related work

The problematic implications of technological advancements for forgetting, forgiving, and reinvention have recently become a policy conversation but have been of concern for privacy scholars since the 1970s when Alan Westin and Michael Baker explained in Databanks in a Free Society, that:

> Many citizens assume, out a variety of religious, humanistic, and psychiatric orientations, that it is socially beneficial to encourage individuals to reform their lives, a process that is impeded when individuals know (or feel) that they will automatically be barred by their past 'mistakes' at each of the later 'gate-keeping' points of social and economic life. Because the computer is assumed not to lose records, to forward them efficiently to new places and organizations, and to create an appetite in organizations for historically complete records, the computer is seen as threatening this forgiveness principle (Westin & Baker, 1972).

In 2002, Jean-Francois Blanchette and Deborah Johnson began discussing how systems can account for forgiveness principles expressed in the American laws of bankruptcy, juvenile criminal records, and credit reporting by categorizing data that will designates its lifespan (permanent, long-term, medium-term, and flash records) (Blanchette & Johnson, 2002). In 2006, Liam Bannon criticized design attributes of computer memory in relation to human memory arguing that forgetfulness is a virtue of memory, not a bug, and should be built into computer memory systems (Bannon, 2006). Martin Dodge and Rob Kitchin (2007) agree, claiming that forgetting should be an integral part of any system and that "the goal is to make the system humane and yet still useful." The authors suggest adding features that mimic absent-mindedness, misattribution, and sporadic blocking (Dodge & Kitchin, 2007). Anita Allen analyzed the legal implications for 'lifelogging,' a total recall movement inspired by Gorden Bell's My Life Bits project, concluding that memory glitches being built into lifelogs protect against its use and misuse by others (Allen, 2008).

[1] Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, and Farnam Jahanian, *Internet Inter-domain Traffic*, In ACM SIGCOMM (2010) (finding 50 percent of Internet traffic is contributed by 150 networks, large companies such as Limelight, Facebook, Google, Microsoft and YouTube generated and consumed 30 percent of all Internet traffic).

[2] While responses to legal requests for information may vary (efforts like Europe v. Facebook, http://europe-v-facebook.org/EN/en.html and #NOLOGs, https://www.privacyinternational.org/blog/what-does-twitter-know-about-its-users-nologs may extend user access to those requests deriving from non-E.U. users, they are not required to), it is expensive and time consuming to design country or region specific systems.

Prior to European Union policy developments, Viktor Mayer-Schönberger's *Delete* put the issue on the table in 2009. Additionally, in 2009 Franz Werro published his article Transatlantic Clash which details the difference between the United States and Swiss treatment of old personal information, specifically analyzing the right to be forgotten and concluding the two cannot be reconciled (Werro, 2009). Since 2009 and the release of the European Commission's intention to bring the right to be forgotten into the Internet Age in 2010 (European Commission, Press Release, 2010), a number of articles have discussed the right to be forgotten and fall within three categories: framing, conceptual development, and conflicts with the U.S. First Amendment. Bert Jaaps Koops covers some history of the subject, draws three conceptual possibilities, and establishes issues that need to be resolved (Koops, 2011). Similarly, Rolf Weber establishes a background for the right, compares U.S. and European treatment in the courts, and places the right to be forgotten with other developments in privacy regulation, concluding with issues that need to be resolved (Weber, 2011). Finally Pere Simon Castellano performs a comparative analysis of treatment of the right to be forgotten by French, Italian, and Spanish data protection agencies, framing why the E.U. DP Regulation seeks to harmonize the right and differences among European countries (Castellano, 2012).

Conceptual arguments that the right should be limited only to user initiated data minimization and meant only to cure the issues with consent online are put forth by Ausloos (2012) and Bernal (2011) emphasizing that the right is only meant to offer more user control in big data practices. On the other end of the spectrum, Xanthoulis (2012) argues that the right should be conceptualized as a human right, not a control right and Andrade (2012) argues that the right should be one of identity, not privacy, stating the right to be forgotten is the "right to convey the public image and identity that one wishes". Eltis (2011) describes the conflicts between civil law and common law concepts surrounding the right in order to help explain the distribution of duties and responsibilities. Finally, Conley (2010) investigates establishing the right within U.S. law concluding it should be conceptualized as a property right.

Thus far, three authors have addressed the conflict between the right to be forgotten with the U.S. First Amendment. Rosen (2012) goes through three scenarios proposed by Google's chief privacy office, Peter Fleischer, and concludes that if the E.U. discontinues the safe harbor agreement with the U.S. currently, "[i]t's hard to imagine that the Internet that results will be as free and open as it is now". After covering the concept of newsworthiness within U.S. tort law, McNealy (2012) applies the right to be forgotten, to a recent case that arose in California and concludes that a right to be forgotten claim would fail because the information would be considered newsworthy and not highly offensive. Walker (2012) similarly concludes that the only right to be forgotten that would be constitutional is a right to delete information voluntarily submitted by the data subject and would require legislative action to create an implied-in-law covenant in contracts to withdraw consent.

Three other articles are outliers; Mitrou and Karyda (2012) argue that privacy enhancing technologies must also be developed to implement the right to be forgotten and Steven C. Bennett (2012), as well asSiry and Schmitz (2012) focus on explaining the jurisdictional issues surrounding the right. Other relevant work has addressed "legal forgiveness" in the U.S. (Ambrose, Friess, & Matre, 2012), outlines of a useful information life cycle (Ambrose, 2013), concepts of information stewardship (Ambrose, 2012), and an organization for possible applications (Ambrose & Ausloos, 2013). While many of the pieces of the puzzle have been put in place through this research, there is still no clear picture. This article builds on the above work and looks specifically at how non-E.U. countries can and should respond to the right to erasure, with the goal of co-regulation or interoperability in mind, as the new DP Regulation continues to be debated and amended.

3. Data protection directive, then and now

As explained above, two distinct concepts of the right to be forgotten, now the right to erasure, emerge from the literature: a right to delete related to control of one's data trail (Bernal, 2011; Ausloos, 2012) and a right to oblivion related to informational self-determination (Andrade, 2012; Xanthoulis, 2012). The right to be forgotten was initially stated to be "strengthened" (European Commission, Press Release, 2010) by the new DP Regulation, suggesting that the DP Directive contained a right to be forgotten, but the recent European Court of Justice Advocate General's opinion explains the many ways it does not (Google Spain SL, Google, Inc. v. Agencia Espanola de Proteccion de Datos (AEPD)).[3]

The difference between the 95′ DP Directive and the proposed DP Regulation in the area of the right to erasure are slight in that it builds off existing data protection rights in the former and significant in that the latter gives the user an explicit right to enforce data rights that result in retroactive deletion without the burden of showing compelling grounds, a process which can be quite difficult in an opaque and complex information landscape. Art. 6(1)(e) DP Directive declares that personal data can be kept "for no longer than is necessary for the purposes for which the data were collected or for which they are further processed". This principle of data minimization places a burden on the data controller to decommission data when it no longer has a legal basis to process, including the completion of the purpose for data collection. Art. 6(1)(e) does not include a user-participation aspect to data minimization; however. Art.12(b) grants the data subject the right to "obtain

[3] On May 13, 2014, the Court of Justice of the European Union (CJEU) handed down its decision that varied dramatically from the Advocate General's opinion, establishing a right to be forgotten based on strongly on Art. 12 (grants the right to rectify, block, or erase further processing of personal data that does not comply with the Directive, particularly if it is inaccurate or incomplete) of the DP Directive. Thus, the DP Regulation does strengthen a right to be forgotten, explicitly granting the right to erase personal information. Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (ECJ 13 May 2014).

from the controller (…) erasure or blocking of data", but only applies "when the processing does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data". Art. 14 provides the data subject a right to object to data processing, but only requires member states to provide a right to object when data collection was legitimate under Art. 7(e) ("tasks of public interest") or 7(f) ("necessary for the legitimate interests of the data controller") *and* if the objection is based on "compelling and legitimate grounds". This means that member states are not bound to introduce a right of objection in cases where data was collected under any of the other three justifications: data subject has given consent, processing is necessary to perform a contract, legal obligation or to protect a vital interest of the data subject (Art.7 (a)–(d)). Additionally, a right to object does not obligate deletion. In conclusion, "These rights can only be invoked when the processing does not comply with the Directive in the first place, i.e., when it is illegal" (Alsenoy, Kuczerawy, & Ausloos, 2013).

The amended DP Regulation would give data subjects the right to delete information about them without all the fuss: no burden to show inaccuracy or compelling grounds. A data controller must delete data that identifies an individual upon request if (a) the purpose limitation principle is breached; (b) consent is withdrawn or legitimate storage period have been exceeded; (c) the right to object to data processing has been legally exercised under Article 19, the right to object (i.e., when processing is based on the its necessity to protect the vital interests of the data subject or for the performance of tasks carried out in the public interest and unequivocally if data is processed based on the legitimate interests of the controller and associated third party); (d) a court or regulatory authority in the E.U. has ruled that the data must be erased; (e) the processing of data is illegal (i.e. does not comply with the Regulation). The first (a) grants a user participation right in data minimization. The second (b) requires the deletion of data when the subject retroactively withdraws consent in consent-based data transfers. The third (c) does not require a relationship between the data controller and data subject; it grants the data subject the right to object, similarly to the 95 DP Directive, but places the burden on the data controller to show that retention is necessary. The last (d) and (e) allows erasure when it does not comply with the Regulation as well as other laws and legal orders.

Additionally, the DP Regulation explicitly grants the data subject the right to erase personal information that has been made public. Art 17., Para. 2 reads:

> Where the controller referred to in paragraph 1 has made the personal data public without a justification based on [legitimate grounds for retaining the data found in] Article 6(1), it shall take all reasonable steps to have the data erased, including by third parties, without prejudice to Article 77[, which refers to the right to compensation and liability]. The controller shall inform the data subject, where possible, of the action taken by the relevant third parties.

When personal data has been made public the original data controller will be responsible and will have to take steps on behalf of the data subject to erase the data.

Of course there are exceptions to erasure in order to strike a balance with other rights. Para. 3 allows the data controller to retain the data for which deletion has been requested if one of four exceptions apply: (a) to protect the right of freedom of expression; (b) for reasons of public interest in the area of public health; (c) for historical, statistical and scientific research purposes; (d) for compliance with a legal obligation to retain the personal data by Union or Member State law.

Although the legislative process is not over and has been heavily debated creating significant doubt, swift adoption of the amendments by the European Parliament and remarks from Reding suggest that data reform is in coming and that it will include a right to erasure (European Commission, Press Release, 2014). The way in which the exceptions to erasure will be applied and balance will be struck is unknown. The European Court has a rich history of case law balancing privacy and expression, but it is unclear how the freedom of expression exception to the right to erasure will be applied, meaning whose balance between privacy and expression will be used to determine the rights of a data subject in relation to those of the data controller and the public.

The DP Regulation differs from the DP Directive in that it sets rules for all E.U. member states as opposed to directing them to enact their own regulations within a set of principles. That being said, each member state will have an active role in interpreting and enforcing these regulations through their own data protection agencies. If the data controller's freedom of expression is to be determined by the jurisprudence of her country, the U.S. may likely prevent many right to erasure claims. More likely, the balance between freedom of expression and privacy will continue to be made by each E.U. country where the claim arises, meaning the right to erasure's freedom of expression exception will be interpreted by E.U. countries saddled with ensuring their citizens are effectively granted these new rights (Kohl, 2007).[4] Eventually such claims the European Court of Justice may hear these claims, but in the meantime, a body of right to erasure jurisprudence does not exist for the E.U.[5] The remainder of this article analyzes how non-E.U. organizations and countries can react to a right to erasure and its exceptions. The exercise tests the existing language to reveal issues of international interoperability. Recognizing that the maintenance of culturally established balances between privacy and expression are important to all involved, it concludes by providing guidance on the right as it takes form in the E.U.

[4] Uta Kohl, Jurisdiction and the Internet 202 (2007), ("In light of [decisions after LICRA v. Yahoo!, Inc. and Yahoo France Tribunal de Grande Instance de Paris, 22 May 2000] from across the globe, this holding is now hardly extraordinary.").

[5] Although the CJEU has decided that a right to be forgotten exists in the DP Directive, jurisprudence guiding the subject is still virtually non-existent and the Court offered little guidance on how to balance relevant interests. Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (ECJ 13 May 2014).

4. Copy and paste

One way to streamline data protection is to adopt universal or harmonized regulation. Universal data protection decreases compliance costs dramatically, but requires homogeneity in values associated with data protection. This section will analyze the possibility of a right to erasure in the U.S. as it is currently articulated by the E.U. DP Regulation. The notion of a right to be forgotten is perceived to be one not well-received in the U.S. However, there are pockets of excitement about such a right in the U.S., but most emphasize the problems associated with persistent data (Bennett, 2012).

The general consensus is that the right to be forgotten would violate the First Amendment. Werro compares the Swiss analog version of the right to be forgotten, which provides the right to preclude anyone from identifying her in relation to her criminal past, with the U.S. public disclosure tort, the closest U.S. equivalent (Werro, 2009). The public disclosure of private facts creates liability for the publication of private facts that are "of a kind that would be highly offensive to a reasonable person, and is not of legitimate concern to the public", (Restatement, 1977). After working through a number of decisions, McNealy (2012), Walker (2012), and Werro (2009) conclude that the public disclosure of private facts tort has established an impossible standard for the right to be forgotten to overcome. In 1975, *Cox Broadcasting v. Cohen* involved a plaintiff who was the parent of a deceased rape victim who was identified by in a broadcast related to the trial of the alleged attacker. The Supreme Court narrowly decided that Cox was not liable for the disclosure of truthful information found in public court records, because "[e]ven the prevailing law of invasion of privacy generally recognizes that the interests in privacy fade when the information involved already appears in the public record". Four years later, the public disclosure tort took another hit when the Court decided *Smith v. Daily Mail*, which involved the identification of a juvenile murder suspect by a newspaper that had learned his identity by interviewing witnesses (1979). The Court again found for the publisher explaining, "If a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." Finally, in *Florida Star v. B.J.F.*, the Court overturned compensatory and punitive damages ordered against a local newspaper that had published the name of a sexual assault victim after reading the name in a police report accidentally placed in the police station pressroom (where signs were up that said the names of sexual offense victims could not be published) (Fla. Star v. B.J.F., 1989).

The Supreme Court left an important opening, stating "we do not hold that truthful publication is automatically constitutionally protected, or that there is no zone of personal privacy within which the State may protect the individual from intrusion by the press", (Fla. Star v. B.J.F., 1989). The right to be forgotten is not equivalent to the public disclosure of private facts tort, but it also does not necessarily slip in that opening. A few U.S. cases are more on point, including Gates v. Discovery Communication Inc. (2004), which overruled an earlier decision finding a publisher liable for a story revealing the criminal past of a man after eleven years of law abiding. Relying on *Cox* and *Florida Star*, the *Gates* court determined that finding liability for the publication of the plaintiff's involvement in a decade-old murder case violated the First Amendment. These cases clearly show that the traditional analog version of the right to be forgotten is not viable under the U.S. constitution. But, these cases were new publications of old information, meaning there is an assumed degree of newsworthiness. Similarly, Melvin v. Reid (1931) and Sidis v. F-R Pub. Corp. (1940) involved dredging up information from the past and disclosing it many years later. In *Sidis* the Second Circuit found a 'where are they now' article about a child prodigy – 20 years after the paper initially covered the boy – was sufficiently newsworthy to gain First Amendment protection, but previously in *Melvin* a former prostitute who was married with a family seven years later successfully sued for invasion of privacy when a movie revealed the details of her past and used her maiden name. More recent and more relevant is the dismissal of a small claims suit brought by the father of a college football player against the editor-in-chief of a newspaper for the intentional infliction of emotional distress. In 2006, the *Daily Californian* published, against the pleas of his parents, a story about the son's suspension from the Berkeley football team because of his actions at an adult club, a downward spiral ensued, and in 2010 he died Purtz v. Srinivasan, 2011. The parents sued after the newspaper refused to remove the article from the website. Its perpetual existence has caused a great deal of emotional pain, but the court found that the two-year statute of limitations in the Uniform Single Publication Act begins upon the first publication as well as problems asserting intentional infliction of emotional distress derived from libel of the memory of a deceased family member. More of these cases will likely be pursued, and jurisprudence will develop to deal with surrounding claims filed by an individual on her own behalf within the statute of limitations for damaging content that remains online and show that the information was no longer of public interest.

The Supreme Court has not been entirely opposed to preventing disclosure or access to old, personal, truthful information that is newsworthy. In DOJ v. Reporters for Freedom of the Press (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). The organization had filed a FOIA request for criminal history records of individuals involved in organized crime and a corrupt congressman from the FBI. 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," (DOJ v. Reporters for Freedom of the Press, 1989). It added, "[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", (DOJ v. Reporters for Freedom of the Press, 1989). Put slightly differently in Rose v. Department of the Air Force (1974), "a person's privacy may be as effectively infringed by reviving dormant memories as by imparting new information", (*see* Department of Justice Guide to the Freedom of Information Act, 2009).

Even if courts were willing to look at 'newsworthiness' in a more nuanced way (requiring continued interest or newsworthiness of the personal information itself), Communications Decency Act § 230 designates "interactive computer services" as distributors, not publishers, of content, thereby exempting them from state tort liability. Sites that host user-generated content without producing content of their own do not have to remove content even when given notice of its defamatory or private nature. This limitation weakens the effectiveness of a right to be forgotten (Walker, 2012).

There may be room for a right to be forgotten in the U.S., but is unlikely to apply to information made publicly available online anytime in the near future. Walker explains that only a limited right to be forgotten is compatible with the First Amendment. The limited right would apply only to data voluntarily submitted and deletion would require legislative action to establish an implied-in-law covenant in contracts between data controllers and data subjects (Walker, 2012). Ausloos proposed a similar limitation, arguing that the right to delete should simply be a withdrawal of consent where it has already been given (2012).

The legal interests associated with data collected through automated surveillance online are far from established, but there has been a general movement to grant users greater rights to participate in how data about them is collected, processed, and used. Many have argued that the E.U. DP Regulation should only grant this type of right to be forgotten: user participation in the principle of data minimization to ensure its deletion after the original purpose for collection has been fulfilled (*see* e.g., Ausloos, 2012; Bernal, 2011). A number of data controllers and services already offer this type of user participation, (*see* e.g., Google Dashboard, BlueKai, Suicide Machine), which is why Jeffrey Rosen (2012) calls this aspect of the right to be forgotten a "non-issue."

More recently, Eugene Volokh, professor at University of California, Los Angeles and academic affiliate of the law firm Mayer Brown, has argued in his capacity as advocate not scholar, that search engines are speakers (Volokh, 2012). According to Volokh, speech exercises by the search engine occur when it conveys information prepared by the search engine itself, reports about others' speech by directing users to material that best suits their queries, includes select excerpts from pages, and selects and sorts results using discretion to determine the most helpful and useful information for the searcher. Essentially the argument is that search engines exercise editorial judgment, similarly to newspapers, and should have the same First Amendment protection in the output of their data processing. Although the technology for information distribution has changed, Volokh argues, "the freedom to distribute, select, and arrange such speech remains the same". Although a highly contested claim, the extension of First Amendment protection to data, indexes, or search results would arouse many of the same censorship arguments that stem from oblivion. However, Neil Richards argues that data may not receive a great deal of First Amendment protection as commercial speech (2013). He assesses a set of cases that address whether the sale of commercial data is 'free speech,' focusing on the 2011 case of *Sorrell v. IMS*, in which the U.S. Supreme Court found that regulating the marketing of data about doctor's prescribing practices violated the First Amendment. The data trade is "much more commercial than expressive" because "[u]nlike news articles, blog posts, or even gossip, which are expressive speech by human beings, the commercial trade in personal data uses information as a commodity traded from one computer to another", (Richards, 2013). In fact, Richards argues that asking whether data is "speech" is the wrong question; the right question is whether the regulation of data flows threatens free speech values.

Jeffrey Rosen asked a similar question when he investigated whether internal practices related to data removal at companies like Google and Twitter foster free speech values (Rosen, 2013). These "delete squads" craft policies to determine what should be removed and what should remain on their sites based on a number of different ethical considerations including legal traditions around the world. These technology leaders could copy and paste the E.U.'s right to erasure into their internal policies, but considering their current resistance to remove user content based solely on request of the user,[6] it is unlikely that the right to erasure will be integrated seamlessly into internal removal practices.

While the outcomes of a right to erasure claim, as either oblivion or deletion, are not entirely clear, an oblivion-style right to erasure claim is more tenuous under U.S. constitutional law and culture than an deletion-style right to be forgotten, which has more public support and legal foundation. Both have uncertain likelihoods of developing in the U.S. without being declared a violation of the First Amendment.

5. Ignore it

Although a number of authors have argued that the right to be forgotten would violate the First Amendment, the unconstitutionality of the right to be forgotten in the U.S. may matter little. When E.U. citizens send requests outside the E.U. to delete information pursuant the right to be forgotten, another option for non-E.U. entities is to simply ignore the right to erasure claim, perhaps because they conflict with the data controller's legal rights within her own country or because there is no way to enforce it. There are of course consequences to such neglect.

According to Bennett, there is some movement toward compromise between the U.S. and E.U., but the approaches do currently conflict (2012). Whether E.U. authorities can regulate and adjudicate activities located outside the E.U. based on their impacts within the E.U. is not clear. This is a very old and very complex conundrum. Jurisdiction is generally based on sovereignty (boundaries and borders), but cyberspace is (semi-)borderless and therefore problematic – an "effects" standard

[6] For instance, Google's policy for removing personal information reads, "Google search results are a reflection of the content publicly available on the web. Search engines can't remove content directly from websites, so removing search results from Google wouldn't remove the content from the web. If you want to remove something from the web, you should contact the webmaster of the site the content is posted on and ask him or her to make a change. Once the content has been removed and Google has noted the update, the information will no longer appear in Google's search results. "FAQ – Policies & Principles – Google", Google, http://www.google.com/policies/faq/.

naturally steps in to substitute for territorial sovereignty, but this approach can lead to unlimited jurisdiction and exposes intermediaries to more liability than the U.S. wishes. The U.S. relies on the "Zippo test," which is a sliding scale for deciding jurisdiction that rests on distinctions between active and passive Internet contacts with a forum state, crafted in Zippo Mfr. Co. v. Zippo Dot Com, Inc. (1997). Passive contacts are those created when a site "does little more than make information available" and create no basis for personal jurisdiction; where active contacts result when the site involves "knowing and repeated transmission of computer files over the Internet" (e.g., doing business with a state over the Internet, entering into contracts with residents, directing content to state residents, etc.) (Zippo Mfr. Co. v. Zippo Dot Com, Inc., 1997).

The E.U. takes a different approach to jurisdiction. It applies E.U. law to any organization that uses means within the E.U. to collect or process personal data even though the DP Directive only purports to govern E.U. entities (Bennett, 2012). It has been suggested by the Article 29 Data Protection Working Party, which advises the E.U. on these issues, that any online interaction with an individual residing in the E.U. may be enough to force compliance with E.U. data protection requirements (Art 29, 2002).

While the E.U. may *say* their laws apply to non-E.U. entities, the countries where non-E.U. entities are established may say otherwise. The possibility of ignoring E.U. laws and court orders hinges on cooperation and enforcement. This area of law is uncertain, due in large part to the now iconic Yahoo! Nazi memorabilia case from 2000 and the subsequent U.S. litigation concluding in 2006, which acknowledged this challenge, "The extent of First Amendment protection of speech accessible solely by those outside the United States is a difficult and, to some degree, unresolved issue…" (Yahoo!, Inc. v. LICRA, 2006).

Briefly, the Tribunal de Grande Instance in Paris ruled against Yahoo! and its French subsidiary after being sued by two anti-racist organizations, LICRA and UEJF, for allowing users in France to view and buy Nazi memorabilia on its auction site. Allowing such communication in France was determined to be a "manifestly illegal disturbance" and the distribution of Nazi paraphernalia (LICRA and UEJF v. Yahoo! Inc., 2000). Yahoo! servers were located in California and the company argued the auction site was intended for U.S. users and that it would be impossible to exclude French users. Yahoo! was ordered to excluded French users from Nazi artifacts and hate speech or suffer a 100,000 francs per-day penalty. The Northern District of California found that it had personal jurisdiction over LICRA, that the claim was ripe, and that enforcement of the French order would be inconsistent with the First Amendment (Yahoo!, Inc. v. LICRA, 2001). On appeal, the Ninth Circuit overturned and dismissed the case, but little clarity was established: 3 found no personal jurisdiction (8 found personal jurisdiction) and 6 found against ripeness (5 in favor of ripeness), which resulted in a six to five majority for dismissal (Yahoo!, Inc. v. LICRA, 2006). While the district court acknowledged that a "basic function of a sovereign state is to determine by law what forms of speech and conduct are acceptable within its borders," it refused to enforce the order on public policy grounds. The Ninth Circuit noted, "Inconsistency with American law is not necessarily enough to prevent recognition and enforcement of a foreign judgment in the United States. The foreign judgment must be, in addition, repugnant to public policy." The majority of the Ninth Circuit agreed that the extraterritorial reach of the First Amendment would not be decided, but the dissent did argue that the order was repugnant to U.S. public policy.

While state[7] and federal[8] anti-libel tourism statutes, prevent (or allow for the prevention of) enforcement of foreign defamation claims that are not at least as protective of free speech as the First Amendment, the same has not been extended to information privacy claims (Bates, 2011). The refusal of enforcement for public policy justifications is available to the courts, but perhaps in the interest of international cooperation, large commercial data controllers generally comply with court orders for privacy violations from foreign jurisdictions or challenge them within the foreign jurisdiction's system.

"Most high-profile online businesses make a determined effort to comply with the laws of targeted States by, for example, having specially tailored sites which are compliant with local law managed by local subsidiaries, even when evasion of local law would easily be possible," by say avoiding physical presence in the targeted country (Kohl, 2007). Google for example, complies with DMCA takedown requests as well as orders to remove speech-related content. Between January and June of 2012, Google removed 992 of the 1026 web search results requested by French court orders (France – Government Removal Requests – Google Transparency Report). Google explains, "Some requests may not be specific enough for us to know what the government wanted us to remove (for example, no URL is listed in the request), and others involve allegations of defamation through informal letters from government agencies, rather than court orders. We generally rely on courts to decide if a statement is defamatory according to local law," (Google Transparency Report, 2013).

Some entities that receive a right to erasure take-down notice could in theory be within the jurisdiction of a European country because the content is accessible by the user in that country, others will be more squarely within the jurisdiction maintaining specifically targeted access, engaging in transactions with the country, or otherwise having a presence in the country. The intent of European countries to make regulatory reaches is unclear. As Bennett explains, "Indeed European case law tends to extend well beyond U.S. views of the reach of jurisdiction, based on Internet activity… In addition to the *Yahoo!* case… and a host of other similar cases, in the recent criminal prosecution of Google executives in Italy, the Italian court held that, because at least some of the information took place in Italy, the court could properly exercise jurisdiction,"

[7] 1962 Uniform Foreign-Country Money Judgments Recognition Act §4(b)(3) allows a court to decline the enforcement of a foreign judgment if the cause of action "on which the judgment is based is repugnant to the public policy of this state…" The 2005 Uniform Foreign-Country Money Judgments Recognition Act §4(c)(3) allows a court to decline the enforcement of a foreign judgment "on which the judgment is based is repugnant to the public policy of the state or of the United States".

[8] The Speech Act of 2010, 28 U.S.C. §4101–4104, "prohibit[s the] recognition and enforcement of foreign defamation judgments and certain foreign judgments against the providers of interactive computer services".

(Bennett, 2012). For those entities that do not want to ignore the right to erasure because it has become an important tenant of European information principles or cannot ignore the right to erasure because enforcement is possible, completely ignoring requests is not a viable option. The penalty for ignoring the DP Regulation is up to 500,000 Euros or up to one percent of annual worldwide income (Art. 79(5)(c), DP Regulation, 2012).[9]

6. Enforce Takedowns

It may not be possible for any data controller who has seizable property in or frequently travels to Europe to simply ignore the right to erasure, but complete compliance with the current formulation of the right could dramatically alter the Internet. As written, the right to erasure functions similarly to the Digital Millennium Copyright Act takedown notice regime (17 U.S.C. § 512), in that it empowers users to initiate take-down action against those that can effectuate the removal. Non-E. U. entities and countries could simply comply with takedown requests. By comparing the issues that have arisen from DMCA takedown requests, it appears this option is quite problematic as well.

Section 512 of the DMCA grants safe harbor from secondary copyright liability (i.e., responsibility for copyright infringement of an end user) to online service providers (OSP) that remove content in response to a takedown (cease-and-desist) notice from the copyright holder. This can be the removal of an image, song, or video or a link that simply directs one to the complained of content. There is no judicial oversight involved in this initial takedown-for-immunity arrangement. Use of copyrighted material may be permitted in situations that are considered fair use, found in Section 107. These exceptions include criticism, comment, news reporting, teaching, scholarship, or research and are subject to a balancing test applied on a fact-specific, case-by-case basis. If a user believes her use of content falls within a fair use exception, she can file a counter-notice, but the OSP is required to keep the content offline for a week (17 U.S.C. § 512(g)).

The DMCA takedown notice system is beneficial for a few reasons: (1) it limits OSP fear of liability and therefore excessive removal of user content; (2) it is arguably less costly and burdensome than intermediary monitoring; and (3) both the notice and counter-notice system are incredibly efficient (Urban & Quilter, 2006). The last one is shared by the right to erasure removal system, which does not have a safe harbor clause and a data controller would not be expected to monitor for data a user may or may not want to be forgotten. It also has the benefit of avoiding the unwanted publicity that filing a privacy claim can bring. A takedown regime for the right to erasure would be cheap, efficient, and privacy-preserving. All a data subject must do is contact a data controller that would exercise removal of the information, and the data must comply unless retention would follow under one of the exceptions. Efficiency comes at a cost, and the DMCA has offered a lesson when it comes to the threat of litigation that hinges on their interpretation of uncertain exceptions.

Wendy Seltzer explains the way takedown system can significantly chill speech. “The frequency of error and its bias against speech represents a structural problem with secondary liability and the DMCA: the DMCA makes it too easy for inappropriate claims of copyright to produce takedown of speech”, (Seltzer, 2010). It is too easy for two main reasons: (1) even good faith claims involve legal uncertainty; (2) speedy removal creates an incentive to file dubious claims (Urban & Quilter, 2006). One study from 2007 found that a third of the DMCA takedown notices in the Chilling Effects database presented obvious questions for a court such as fair use determination or the legitimacy of the copyright. Additionally, 57% of notices were sent to target content of a competitor (Urban & Quilter, 2006).[10] While not substantially effective, the DMCA does include safeguards to prevent abuse such as penalties for misrepresenting content or activity as infringing (17 U.S.C. § 512(f)). The right to erasure has no such safeguards.

The potential for abuse in user initiated takedown systems is already incredibly high, but the added element of international uncertainty regarding the interpretation of the right to erasure and its exceptions make widespread abuse inevitable. The right to erasure is vaguely written with broad exceptions and void of jurisprudence. Arguably every right to erasure takedown request would involve a substantive legal question related to the underlying claim.

7. Middle ground

Regulators and researchers have long recognized that harmonizing international data protection is a priority for the vitality of the international Internet economy, which is how the “safe harbor” arrangement with the U.S. Dept of Commerce came about (Department of Commerce, 2000). Establishing minimum standards or co-regulation is important, but as the Fair Information Practices Principles has exemplified, the devil is in the details. In his book *Jurisdiction and the Internet*, Uta Kohl bluntly states that “regulators are faced with a very simple choice: either make law more transnational or online activity less transnational. And this is *always* the only choice: there is no middle way, no gray between the black and the white”, (Kohl, 2007). The right to be erasure must utilize both. A right to erasure that establishes a harmonized balance between privacy and expression (i.e., applies the freedom of expression exception the same transnationally) is simply not

[9] DP Regulation, Art. 79(5)(c), (“The supervisory authority shall impose a fine up to 500 000 EUR, or in case of an enterprise up to 1% of its annual worldwide turnover, to anyone who, intentionally or negligently: does not comply with the right to be forgotten or to erasure, or fails to put mechanisms in place to ensure that the time limits are observed or does not take all necessary steps to inform third parties that a data subjects requests to erase any links to, or copy or replication of the personal data pursuant Article 17.”)

[10] The database only included seven counter-notices, which is not an accurate representation of responses to the takedown notices as these are automatically contributed to the Chilling Effect database.

currently possible. It ignores the particular national values that have resulted in divergent laws. However, that does not mean that country specific sites or treatment needs to be created by every data controller, but that data controllers be responsive when that balance has been made by different national governments. In other words, regulatory cooperation, as opposed to harmonization, must be forged on this subject.

However, regulatory harmonization may be possible for the regulation of passively created, privately held data (the right to erasure) and should be embraced. In order to harmonize this aspect of the right to erasure, deletion must be separated from oblivion. As I have argued previously, the DP Regulation currently condenses the two and treats them similarly, which is inappropriate because of the different interests associated with the retention of privately-held versus publicly available information. If the right to erasure was separated from the right to oblivion, the existing Art. 17 would be much less problematic. Many versions of FIPPs already include the principles of data minimization and user participation (Gellman, 2012), and Art. 17, Para. 1 essentially grants users a right to participate in and enforce data minimization principles, as well as the withdrawal of consent to retroactively cure issues of informed consent in an online environment. Additionally, some platforms already offer this service to users, including Google dashboard. The Network Advertising Initiative allows users to opt-out of receiving targeted advertisements from its 98 member companies (Network Advertising Initiative), Spokeo allows users to opt-out of being listed (Spokeo, 2011), and the World Wide Web Consortium continues to work to develop a "Do Not Track" mechanism (Electronic Frontier Foundation). Still, often users must delete accounts in order to delete data (Facebook, 2012).[11] Neither an opt-out mechanism that prevents future collection nor requiring a user to fully delete an account in order to delete data will likely meet a right to erasure standard. It will require creating means for real user access and participation in data processing practices, which is of course challenging, but generally agreed upon (Department of Commerce 2010).[12] As noted above, this type of data also may receive less protection as commercial speech (Richards, 2013).

Art. 17, Para. 2 provides procedures for the removal of information that has been made publicly available. This aspect of the proposed Regulation relates to the right to oblivion – the way in which information that is easily accessible online impacts reputation, self-perception, second chances, and transformation. The values associated with publicly available information are different than those associated with privately held data, particularly if it is commercial (Ambrose & Ausloos, 2013; Ambrose, 2013). The right to oblivion (the right to remove information made available to the public) will likely have conflict with tenets of free speech. Consequences would be limited significantly by mitigating abuse that will result from user initiated takedown system.

Expression is balanced with privacy very differently across countries. These differences are embodied in different legislative, administrative, and judicial determinations. Again, the DP Regulation intends to create consistency, but how much unclear, and there are no guiding principles in place, except those from member states with widely varying interpretations of the right. The data subjects and data controllers will be trying to determine what should be forgotten and what qualifies as free speech under the right to erasure for the jurisdiction where the request originates. This has been problematic for users responding to DMCA takedown notices, which has a relatively consistent body of legal decisions offering at least some guidance.

Variation between member states has already started to develop, while other countries will be starting from scratch. For instance, the French Commission Nationale de l'informatique et des Libertés (CNIL) pioneered the digital right to be forgotten le droit à l'oubli by placing it within data quality principles (records must be kept accurate, complete, current, and disposed of when no longer necessary), moving the right into the Internet context smoothly (Castellano, 2012). But, in 2011, the French parliamentary commission found that the key concepts of the right to be forgotten, while an attractive concept, was already covered by existing law (the user right to access and require deletion of personal data) and that a new right to be forgotten was not necessary (Wolf, 2011). The Italian Garante per la Protezione dei Dati Personali resolved a diritto all'oblio case in 2004 by recognizing the existence of a right to be forgotten within Art. 11 of the Italian data protection law, specifically its data quality principle (a tool for enforcing purpose specific data minimization) (Castellano, 2012). The Spanish Agencia Española de Protección de Datos (AEPD) also recognizes the right to be forgotten as part of data protection principles of data quality and data minimization and has pioneered a 'new' right to be forgotten. This new form is a right granted to a citizen who has neither public personality status nor subject of a newsworthy event of public relevance to correct or react to the inclusion of personally identifiable information on the internet. Of course, search engines are inevitably implicated,[13] and so AEPD has ordered Google to remove links to sites that disclose out of date or inaccurate personal information, which it deems breaches the right to be forgotten.

A take-down system between data controllers and data subject seeking to be forgotten is not advisable, particularly in such an uncertain legal landscape with variation in the balance between privacy and speech amongst member states.

[11] *See* "Facebook Data Use Policy", Facebook (2012), available at https://www.facebook.com/full_data_use_policy (The policy includes a number of clauses including: "While you are allowing us to use the information we receive about you, you always own all of your information"; We store data for as long as it is necessary to provide products and services to you and others, including those described above. Typically, information associated with your account will be kept until your account is deleted"; "It typically takes about one month to delete an account, but some information may remain in backup copies and logs for up to 90 days.").

[12] *See e.g.*, "Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework," Department of Commerce (2010), available at http://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovationinternet-economy-dynamic-policy-framework. (proposed the following set of FIPPs: transparency, *individual participation*, purpose specification, *data minimization*, use limitation, data quality and integrity, security, and accountability and auditing).

[13] How search engines are implicated under the DP Directive and their future under the DP Regulation is discussed in detail by Brendan Van Alsenoy, Aleksandra Kuczerawy, & Jef Ausloos, *Search Engines after 'Google* Spain': *Internet@Liberty or Privacy@Peril?*, Telecommunications Policy Research Conference (2013).

Instead when information is made public, a court order should be required for right to erasure removal requests. For U.S. sites and services that receive CDA §230 protection in the U.S., dealing with liability in countries where they receive no such immunity is difficult, but as the Google Transparency Report shows, they are capable of handling these orders. Responding to user takedown requests will be incredibly disruptive to operations for sites and services around the world – determining validity, authentication, and country-specific legal interpretation of each claim will be so time-consuming, costly, and inconsistent that many will just remove content automatically. Requiring a court order would allow a body of law to develop for each jurisdiction. It would preserve the different prioritization of privacy and other interests among countries and be less disruptive to sites, services, and information that the world has come to rely on.

8. Conclusion

The world has a stake in information on the Internet. The E.U. has proposed, debated, and amended a right to erasure for its citizens that would allow them to contact a data controller to request the removal of information about them. Non-E.U. countries and data controllers have four options, which show how and where more reform is necessary. First, they can simply harmonize their own laws with the E.U. This option is not realistic at least in the U.S. where the First Amendment likely does not leave room for a right to erasure. Second, they could ignore right to erasure requests. Many companies with a physical presence or assets in the E.U. will not be able to do this because enforcement against those organizations is possible as many others will be within the jurisdiction of E.U. member countries because they transact and direct content at those countries. Whether U.S. courts will enforce orders from the E.U. for ignoring right to erasure claims is not clear, but there may be negative consequences for the U.S. if it chooses not to cooperate. Generally, sites and services want to comply with laws, and so they could simply comply with right to erasure requests as a third option. As a comparison with the DMCA takedown system and results shows, this would likely lead to widespread abuse, serious disruption to site and service operations, and the removal of an unacceptable amount of content. Finally, non-E.U. entities could push for a right to erasure that maintains cultural differences embodied in laws that balance privacy and free speech that does not disrupt the way in which these differences have been handled before, specifically user initiated deletion of information privately held by data controllers and court orders for information publicly available online.

The world will be getting guidance from the way in which Europe will interpret the right to be forgotten when the European Court of Justice decides whether a number of orders from the Spanish AEPD will be enforced (Data Guidance, 2012).[14] The decision, while only in the advisory state, has articulated an interpretation of "data controller" that would not obligate search engines to delete content under the DP Directive and explained that there is no right to be forgotten in the DP Directive (Google Spain SL, Google, Inc. v. Agencia Espanola de Proteccion de Datos (AEPD)).[15] This is the appropriate series of events for interpreting rights – legislation, claims, orders, and judicial interpretation. The DP Regulation draft of the right to erasure dangerously conflates two concepts: the right to delete data collected and privately held and the right to oblivion for information that affects the data subject's public reputation and identity. The two should be treated differently based on the interests involved. It is unclear how and to what extent the right to erasure, if established across the European Union, will be invoked. Its impact on the economics of the internet and business models currently in place will depend on how it is utilized by data subjects, responded to by controllers, and enforced by governments, as well as the adaptability of these commercial entities. Unlike a "do not track" option, the right to erasure allows for data participation in a less systematic way, erasing only what a subject finds objectionable to be removed as opposed to deleting by default.

Harmonization is possible for user participation in enforcing data minimization principles. However, the user initiated takedown system for a right (that has very little legal precedent, with treatment that will vary drastically from jurisdiction to jurisdiction, and involves the removal of information publicly available online) has the potential for abuse that could wreak havoc on the store of information held on the Internet.

Acknowledgments

I would like to thank those at the Telecommunications Policy Research Conference for their feedback and insights.

References

Allen, Anita (2008). Dredging up the past: Lifelogging, memory and surveillance. *University of Chicago Law Review*, 47.

Alsenoy, Brendan Van, Kuczerawy, Aleksandra, & Ausloos, Jef (2013). Search engines after 'Google Spain': Internet@Liberty or Privacy@Peril?. *Telecommunications Policy Research Conference*

Ambrose, Meg Leta (2012). You are what Google says you are: The right to be forgotten and information stewardship. *International Review of Information Ethics*

[14] "E.U. Spain Consults CJEU on Extent of the Right to be Forgotten", Data Guidance (2012), available at http://www.dataguidance.com/news.asp?id=1745.

[15] This aspect of the Advocate General's interpretation was particularly in opposition to the CJEU ruling, which easily found that Google's search activities qualified it as a data controller because it determined the purpose and means of processing the personal data. Case C-131/12, Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González (ECJ 13 May 2014).

Ambrose, Meg Leta (2013). It's about time: Privacy, information lifecycles, and the right to be forgotten. *Stanford Technology Law Review*, 369.
Ambrose, Meg Leta, & Ausloos, Jef (2013). The right to be forgotten across the pond. *Journal of Information Policy*, 1–23.
Ambrose, Meg Leta, Friess, Nicole, & Matre, Jill Van (2012). Seeking digital redemption: The future of forgiveness in the internet age. *Santa Clara Computer& High Tech. L.J.*, 99.
Andrade, Norberto Nuno Gomes de (2012). Oblivion: The right to be different … from Oneself – reproposing the right to be forgotten. *IDP*, 122.
Art 29 (May 30, 2002). Data Protection Working Party. *Working document on determining the international application of E.U. Data Protection Law to personal data processing on the internet by Non-E.U. based web sites*. 5035/01/EN/Final. WP 56.
Ausloos, Jef (2012). The 'Right to be Forgotten' – Worth remembering?. *Computer Law & Security Review*, 143.
Bannon, Liam J. (2006). Forgetting as a feature, not a bug: The duality of memory and implications for ubiquitous computing. *2:01 CoDesign: International Journal of CoCreation in Design and the Arts*, 3.
Bates, Stephen (2011). More SPEECH preempting privacy tourism. *Hastings Communications and Entertainment Law Journal*, 379.
Bennett, Steven C. (2012). The "Right to be Forgotten": Reconciling EU and US perspectives. *Berkeley Journal of International Law*, 161.
Bernal, Paul A. (2011). A right to delete?. *2:2 European Journal of Law and Technology*
Blanchette, Jean-Francois, & Johnson, Deborah G. (2002). Data retention and the panoptic society: The social benefits of forgetfulness. *18:1 The Information Society*
Castellano, Pere Simon (2012). The right to be forgotten under European law: A constitutional debate. *16:1 Lex Electronica*
Christopher Wolf, (July 4, 2011). French Parliamentary Commission Recommends Privacy Law Reform Citing Testimony of Hogan Lovells Privacy Lawyer. *Chronicle of Data Protection, Hogan Lovells*, ⟨http://www.hldataprotection.com/2011/07/articles/international-eu-privacy/french-parliamentary-commission-recommends-privacy-law-reform-citing-testimony-of-hogan-lovells-privacy-lawyer/⟩.
Commercial Data Privacy and Innovation in the Internet Economy: Dynamic Policy Framework, (December 2010). Department of Commerce.
Communications Decency Act of 1996, 47 U.S.C. § 230.
Conley, Chris (2010). The right to delete. *AAAI Spring Symposium: Intelligent Information Privacy Management*
Consumer Opt-OutINAI: Network Advertising Initiative. Network advertising initiative, available at ⟨http://www.networkadvertising.org/choices/#completed⟩.
Cox Broadcasting v. Cohn, 420 U.S. 469 (1975).
Craig Labovitz, Scott Iekel-Johnson, Danny McPherson, Jon Oberheide, & Farnam Jahanian, (2010). Internet inter-domain traffic. In ACM SIGCOMM.
Data Protection Reform – Frequently Asked Questions. (November 4, 2010). *European Commission*, ⟨http://europa.eu/rapid/press-release_MEMO-10-542_en.htm⟩ (last visited 14.10.13).
Department of Justice Guide to the Freedom of Information Act (2009). Department of Justice, 579, available at ⟨http://www.justice.gov/oip/foia_guide09/exemption7c.pdf⟩, *citing DOJ v. Reporters Committee for Freedom of the Press* (1989), 489 U.S. 749, 767.
Dodge, Martin, & Kitchin, Rob (2007). Outlines of a world coming into existence: Pervasive computing and the ethics of forgetting. *34:3 Environment and Planning B-Planning & Design*, *431*, 446.
Do Not TrackIElectronic Frontier Foundation. Electronic Frontier Foundation, available at ⟨https://www.eff.org/issues/do-not-track⟩.
DOJ v. Reporters for Freedom of the Press, 489 U.S. 749 (1989).
DP Directive (October 24, 1995). *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281*. European Commission.
DP Regulation, (January 25, 2012). *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)*. COM (2012) 11 final. European Commission, available at ⟨http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF⟩.
Eltis, Karen (2011). Breaking through the "tower of babel": A "Right to be forgotten" and how Trans-systemic thinking can help reconceptualize privacy harm in the age of analytics. *22:1 Fordham Intellectual Property Media & Entertainment Law Journal*
Eugene Volokh, (August 20, 2012). *Google: First Amendment Protection for Search Engine Search Results*, Vol. 5, available at ⟨http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf⟩.
Europe v. Facebook, ⟨http://europe-v-facebook.org/EN/en.html⟩.
E.U. Spain Consults CJEU on Extent of the Right to be Forgotten, (March 3, 2012). *Data Guidance*, available at ⟨http://www.dataguidance.com/news.asp?id=1745⟩.
Facebook Data Use Policy. Facebook (December 11, 2012), available at ⟨https://www.facebook.com/full_data_use_policy⟩.
Fla. Star v. B.J.F., 491 U.S. 524 (1989).
FAQ – Policies & Principles – Google. Google, ⟨http://www.google.com/policies/faq/⟩.
France – Government Removal Requests – Google Transparency Report, Google, ⟨http://www.google.com/transparencyreport/removals/government/FR/⟩.
Gates v. Discovery Communication Inc., 101 P.3d 552 (Cal. 2004).
Google Spain SL, (June 25, 2013). *Google, Inc. v. Agencia Espanola de Proteccion de Datos (AEPD)*. Mario Costeja Gonzalez, Case C-131/12. Opinion of Advocate General Jaaskinen.
Government Removal Requests - Google Transparency Report, Google, ⟨http://www.google.com/transparencyreport/removals/government/⟩.
How Our Opt-Out System Works « Spokeo People Search Blog, Spokeo (January 12, 2011), available at ⟨http://www.spokeo.com/blog/2011/01/how-spokeo-opt-out-system-works⟩.
Koops, Bert Jaap (2011). Forgetting footprints, shunning shadows. A critical analysis of the "Right to be Forgotten" in big data practice. *8:3 Scripted*.
LICRA and UEJF v. Yahoo! Inc. and Yahoo France (Tribunal de Grande Instance de Paris, 22 May 2000).
Lilian Mitrou & Maria Karyda, (June 29–30, 2012). EU's Data Protection Reform and the Right to be Forgotten: A Legal Response to a Technological Challenge? In *Proceedings of the 5th international conference of information law and ethics* 2012. Corfu-Greece , available at ⟨http://www.google.com/url?q=http%3A%2F%2Fpapers.ssrn.com%2Fsol3%2Fpapers.cfm%3Fabstract_id%3D2165245&sa=D&sntz=1&usg=AFQjCNFSz9htD6UVREfA3FYm1SPwrjHtbg⟩.
McNealy, Jasmine E. (2012). The emerging conflict between newsworthiness and the right to be forgotten. *Northern Kentucky Law Review*, 119. ⟨http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:62012CC0131:EN:HTML⟩.
Melvin v. Reid, 297 Pac. 91 (Cal. App. 1931).
Napoleon Xanthoulis, (2012). Conceptualising a right to oblivion in the digital world: A human rights-based approach. Working paper series, available at SSRN: ⟨http://ssrn.com/abstract=2064503⟩.
Press Release (text of Viviane Reding speech), (June 22, 2010). *European Commission*, available at ⟨http://europa.eu/rapid/pressReleaseAction.do?reference=SPEECH/10/327⟩.
Press Release (text of Viviane Reding speech), (March 16, 2011). *European Commission*, available at ⟨http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/11/183⟩.
Press Release (text of Viviane Reding speech), (January 28, 2014). *European Commission*, available at ⟨http://europa.eu/rapid/press-release_SPEECH-14-62_en.htm⟩.
Purtz v. Srinivasan, (January 11, 2011). No. 10CESC02211. *Fresno Co. Small Cl. Ct.* , available at ⟨http://banweb.co.fresno.ca.us/cprodsnp/ck_public_qry_doct.cp_dktrpt_frames?backto=P&case_id=10CESC02211&begin_date=&end_date⟩ (text of the Statement of Decision, including the judge's personal comments, can be found in the docket entry listed for Jan. 11, 2011).
Restatement (Second) of Torts § 652D (1977).
Richards, Neil (2013). Data privacy and the right to be forgotten after sorrell. *Privacy Law Scholars Conference*
Robert Gellman, (November 12, 2012). *Fair Information Practices: A Basic History*. Version 1.91, available at ⟨http://bobgellman.com/rg-docs/rg-FIPShistory.pdf⟩.
Robert Kirk Walker (2012). Forcing *Forgetfulness: Data Privacy, Free Speech, and the "Right to be Forgotten*". Working Paper series, available at SSRN: ⟨http://ssrn.com/abstract=2017967⟩.
Rose v. Department of the Air Force, 495 F. 2d 261 (2d Cir. 1974).

Rosen, Jeffrey (2012). The right to be forgotten. *Stanford Law Review*, 92 (Online 88).
Rosen, Jeffrey (2013). The delete squad: Google, Twitter, Facebook and the New Global Battle Over the Future of Free Speech. *New Republic*
Safe Harbor Privacy Principles, *U.S. Department of Commerce* (July 21, 2000), available at ⟨http://export.gov/safeharbor/eu/eg_main_018475.asp⟩. U.S.-EU Safe Harbor Framework Documents, available at ⟨http://export.gov/safeharbor/eu/eg_main_018493.asp⟩.
Seltzer, Wendy (2010). Free speech unmoored in copyright's safe harbor: Chilling effects of the DMCA on the first amendment. *24 Harvard Journal of Law & Technology*, 177–178.
Sidis v. F-R Pub. Corp., 113F.2d 806 (2d Cir. 1940).
Siry, Lawrence, & Schmitz, Sandra (2012). A right to be forgotten? How recent developments in germany may affect the internet publishers in the us. *3:1 European Journal of Law and Technology* (available at)
Smith v. Daily Mail Publ'ing, 443 U.S. 97 (1979).
Sorrell v. IMS Health Inc., et al., (2011). 131 S.Ct. 2653.
The Speech Act of 2010, 28 U.S.C. §4101-4104.
Suzanne Daley, (August 9, 2011). *On Its Own. Europe Backs Web Privacy Fights*. The New York Times, sec. World/Europe, available at ⟨http://www.nytimes.com/2011/08/10/world/europe/10spain.html⟩.
Uniform Foreign-Country Money Judgments Recognition Act of 1962, 13 U.L.A. 261 (1986).
Uniform Foreign-Country Money Judgments Recognition Act of 2005, 13 U.L.A. pt. II (2007).
Urban, Jennifer, & Quilter, Laura (2006). Efficient process or "chilling effects"? Takedown notices under Section 512 of the Digital Millennium Copyright Act. *Santa Clara Computer & High Technology LawJournal*, 625 (621).
Uta Kohl, (2007). *Jurisdiction and the Internet: Regulatory competence over online activity*.
Viktor Mayer-Schönberger, Delete: The Virtue of Forgetting in the Digital Age (2009).
Weber, Rolf H. (2011). The right to be forgotten: More than a Pandora's box?. *JIPItec*, 120.
Werro, Franz (2009). The right to inform v. the right to be forgotten: A transatlantic clash. *In Liability in the Third Millennium*
Westin, Alan F., & Baker, Michael A. (1972). *Databanks in a Free Society*, *267*.
Yahoo!, Inc. v. LICRA, 433 F.3d 1199, 1217 (9th Cir. 2006).
Yahoo!, Inc. v. LICRA, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).
Zippo Mfr. Co. v. Zippo Dot Com, Inc. 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).