THE RIGHT TO BE FORGOTTEN

Michael J. Kelly*
David Satola**

The right to be forgotten refers to the ability of individuals to erase, limit, delink, delete, or correct personal information on the Internet that is misleading, embarrassing, irrelevant, or anachronistic. This legal right was cast into the spotlight by the European Court of Justice decision in the Google Spain case, confirming it as a matter of EU law. This “right,” however, has existed in many forms around the world, usually applying a balance-of-rights analysis between the right to privacy and the right to freedom of expression. The new European version, though, is based on a legal theory of intermediary liability where Internet search engines are now considered “data controllers.”
and as such have liability for managing some content online. As it has evolved in Europe, this right has focused attention on key underlying policy considerations, as well as practical difficulties, in implementation under the new European regime. In particular, shifting the burden of creating compliance regimes and supervising important human rights from government to the private sector. Thus, in Europe, the function of balancing rights (privacy versus speech) in the digital context has been "outsourced" to the private sector. Recent experience in Europe under this regime shows that there is no uniform approach across countries. Moreover, different national approaches to the "right" make it almost impossible for multinational entities to comply across jurisdictions. Apart from the data controller threshold, civil-law jurisdictions seem to give greater weight to privacy concerns in striking this balance. Common-law jurisdictions tend to give greater weight to expression. The right to be forgotten, thus, is another example of an evolving transatlantic data struggle with potentially serious trade implications. This Article explores the historical and theoretical foundations of the right to be forgotten and assesses practical legal issues including whether North American "free speech" rights are an effective buffer to what is sometimes a very controversial and evolving issue.

TABLE OF CONTENTS

I. INTRODUCTION ................................................. 3
II. THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION........ 5
   A. The Directives .............................................. 5
   B. The ECJ Decision ......................................... 6
III. COMPLIANCE EFFORTS UNDER THE NEW EU REGIME ............ 16
    A. Implementation Criteria .................................... 17
    B. Implementation Results ..................................... 17
    C. Implementation Territorial Effect ......................... 20
IV. OTHER NATIONAL ANTECEDENTS AND ANALOGIES ............... 22
    A. In Continental Europe ..................................... 23
    B. In Latin America ........................................... 27
    C. In North America ............................................ 31
V. THE BRITISH RESPONSE ......................................... 34
    A. Pre-Brexit Response ......................................... 34
    B. Post-Brexit Possibilities .................................. 36
VI. FREE SPEECH: A CONSTITUTIONAL BUFFER? .................... 38
VII. CONCLUSION .................................................. 50
VII. APPENDICES .................................................. 52
I. INTRODUCTION

"On the Internet, no one knows you’re a dog.” Or do they? Much has changed since this iconic cartoon ran in The New Yorker in 1993, including the degree to which a simple Internet search can return vast amounts of surprisingly detailed information. Since March 2014, our canine friends in Europe can petition search providers there to have this embarrassing fact about them expunged from search results seeking that specific information (likely to the consternation of many cats). North American dogs, however, have no similar legal recourse. What is a dog in Des Moines to do?

This Article explores the reaches of the recent European Court of Justice (“ECJ”) case confirming that such a right now firmly exists within the European Union (“EU”), that EU citizens may avail themselves of it, and that Internet-search providers, such as Google, must comply. In so doing, we explore the legal content of the right: its importance, impact, historical antecedents, and efforts by industry to implement it. Finally, we analyze whether the right to be forgotten is destined to cross the Atlantic and find its way into North American law, or whether traditional judicial preferences in Canada and the United States, favoring freedom of speech over privacy, erect a sufficient constitutional buffer to the wholesale importation of this right.

The “right to be forgotten” refers to the right of an individual to erase, limit, or alter past records that can be misleading, redundant, anachronistic, embarrassing, or contain irrelevant data associated with the person, likely by name, so that those past records do not continue to impede present perceptions of that individual. Although a new arrow in the quiver of privacy-rights advocates, the right to be forgotten is not precisely the same as a traditional right to privacy, which depends on framing a protected interest against the actions of an infringing party such as a government. Moreover, it should not be confused with the right to correct information, or the truth—which is amply protected by centuries of libel and slander jurisprudence. Its aim, rather, is to make certain

---


2. Case C-131/12, Google Spain v. Agencia de Protección de Datos (AEPD), 2014 EUR-Lex (May 13, 2014) [hereinafter Google Spain]. The main issue in the case implicated the obligations of Internet search engines related to the protection of personal data published on third-party websites. Id. at ¶ 20. The ECJ was petitioned to consider a preliminary ruling on the correct interpretation of Articles 2(b), 2(d), 4(1)(a), 12(b), and 14(a) of EC Directive 95/46/EC and Article 8 of the Charter of Fundamental Rights of the European Union (“EU Charter”). See infra Part II.

that information more difficult to find. In that sense, the right to be forgotten, when implemented, is a forced omission.

This right developed in its present form due to technology; or, more precisely, as a response to technology. By 2015, algorithms perfected and deployed by Internet-search providers transformed the information superhighway. Users are able to accurately locate with lightning speed the material they seek, cross-reference what they find to other searches, and gain a complete picture of what they want to know in hours or minutes. Compare with the hours, or even days, that running the same search at a library in 1985 would entail: roving among shelves of books and newspapers, and perhaps poring through microfiche—the best technology of the day—if one was lucky.

As currently articulated in the EU, the right to be forgotten transports those seeking information from the computer age back to the microfiche age on a search-by-search basis. It does so purposely in order to protect the target of the search. The ECJ judgment made clear that, on balance, the right of the "searched" can outweigh the right of the searcher. Importantly, the data about the target is not digitally wiped from the Internet. It still exists. It is, however, much more difficult to find. Hence the frustrating microfiche metaphor: undertaking potentially multiple searches on multiple platforms to locate information slows down the search process significantly. Most Internet users today do not have the patience for this. And that voilà moment that happens when a searcher finally locates what they are seeking after a particularly grueling process is not a sufficiently satisfying emotional cookie to make it worth the effort for most searchers.

The EU's embrace of this right, and the overwhelmingly negative response by the U.K. House of Lords European Union Committee ("House of Lords"), offer convenient counterpoints to consider the implications of this right. In response to criticism leveled against the right to be forgotten, the European Commission said:

"[t]he right to be forgotten is about making sure that the people themselves—not algorithms—decide what information is available about them online when their name is entered in a search engine . . . . It is about making sure that citizens are in control of their personal data. A citizen should be able to have his or her personal data removed from a search engine, if certain conditions are met."

In contrast, the House of Lords repudiated the ECJ decision interpreting EU law, affirming the right's existence, and compelling its enforcement, noting that "[o]nce information is lawfully in the public domain it is impossible to compel its removal, and very little can be done to


prevent it spreading." The House of Lords further remarked that the ECJ decision is "misguided in principle and unworkable in practice," and a "judgment that cannot be complied with brings the law into dispute."

II. THE RIGHT TO BE FORGOTTEN IN THE EUROPEAN UNION

A. The Directives

Directives 2000/31/EC ("2000 Directive") and 95/46/EC ("1995 Directive") form the legal basis of a search provider's obligation to erase links in the European Union. Article 1 of the 1995 Directive articulates the EU's position on privacy rights: "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data." It goes on to regulate the processing of and access to personal data of individuals within the EU. The 2000 Directive seeks to break down electronic barriers to the EU's internal market, and as such, it seeks to rely on the 1995 Directive to regulate personal data.

Nevertheless, both directives work in tandem. The 2000 Directive states that Internet intermediaries, defined as a "mere conduit," are free from liability, but "[i]his Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement." This general scheme of exemption, together with injunctive relief, is similarly applied to "caching" services and "hosting" services. The specific law governing injunctions on these intermediary services depends on the domestic law of Member States, with some coun-

---

6. EUROPEAN UNION COMM., supra note 4, at ¶ 5.
7. Id. at ¶¶ 24, 62.
10. See id. at art. 1. Without so stating, one could argue, under a U.S. constitutional lens, that the 1995 Directive prefers protections of personal privacy to protections of what is known in the United States as "free speech."
11. See Directive 2000/31/EC, supra note 8, at art. 14. "The protection of individuals with regard to the processing of personal data is solely governed by [the 1995 Directive] . . . are fully applicable to information society services; these Directives already establish a Community legal framework in the field of personal data and therefore it is not necessary to cover this issue in this Directive in order to ensure the smooth functioning of the internal market, in particular the free movement of personal data between Member States; the implementation and application of this Directive should be made in full compliance with the principles relating to the protection of personal data, in particular as regards unsolicited commercial communication and the liability of intermediaries; this Directive cannot prevent the anonymous use of open networks such as the Internet." Id.
12. Id. at art. 12(3).
13. See id. at arts. 13(2), 14(3). "This Article shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement." Id.
tries relying on tests typical in general court practice and other countries adopting specific tests.

B. The ECJ Decision

In Google Spain v. AEPD, the ECJ brought together these directives to form the legal basis for a clear articulation of a right to be forgotten.\(^{14}\) The Court explained the interaction of provisions under the 1995 Directive, thus opening a question as to whether exemptions of liability rules could be available to a search engine under the 2000 Directive.\(^{15}\)

The dispute involved Costeja González, a Spanish national, complaining to the Spanish Data Protection Agency (“AEPD”) about the La Vanguardia newspaper retaining two Internet stories linking his name with attachment proceedings in a real-estate auction related to recovery of social-security debts.\(^{16}\) Mr. Costeja requested that La Vanguardia remove or alter the pages or have Google Spain or Google Inc. remove or conceal the personal data in search results.\(^{17}\) AEPD rejected the request with respect to La Vanguardia, but stated that Google Spain and Google Inc. have the power to withdraw the data from search results.\(^{18}\) Google Spain and Google Inc. objected and brought an action before the Spanish National High Court, which stayed the proceedings amid the request to the ECJ.\(^{19}\) The ECJ decided that Mr. Costeja had the right to make this request and have the request reviewed.\(^{20}\)

In the EU judicial system, the Advocate General (“AG”) typically develops the case for the Court and the Court has the AG’s independent analysis in a dossier that they may consider, in addition to the submissions by the parties and other interested parties, such as EU member states, that may seek to intervene in a particular case. In this case, the AG Jääskinen found in his 2013 opinion that Google should not be required to implement a right to be forgotten under the terms of existing EU law.\(^{21}\) Reflecting on the 1995 Directive in light of the then-existing basis of technology, the AG stated:

[w]hen the Directive was adopted the World Wide Web had barely become a reality, and search engines were at their nascent stage. The provisions of the Directive simply do not take into account the fact that enormous masses of decentrally hosted electronic documents and files are accessible from anywhere on the globe and that their contents can be copied and analysed and disseminated by part-

---

14. Google Spain, supra note 2, at ¶ 100.
15. Id.
16. Id. at ¶ 14.
17. Id.
18. Id. at ¶ 16.
19. Id. at ¶¶ 16-20.
20. Id. at ¶¶ 14-15, 98-99.
ties having no relation whatsoever to their authors or those who have uploaded them onto a host server connected to the internet.\textsuperscript{22}

Consequently, the AG determined that a national data protection authority cannot demand that an Internet-search-service provider take personal data out of its index, unless it had ignored exclusion codes or was asked to update its cache memory data.\textsuperscript{23} The AG also considered whether Google was acting as a data “controller,” concluding that Google did not meet the definition of a “data controller” under the 1995 Directive because it was merely gathering data and therefore was not responsible for deleting any data.\textsuperscript{24} The AG concluded that the current data protection rules “[did] not entitle a person to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests.”\textsuperscript{25}

Google welcomed the AG findings.\textsuperscript{26} The AG’s opinion, however, was not followed by the ECJ. By linking together several legal provisions, the ECJ successfully lodged a right to be forgotten in the language of existing EU law—thereby disagreeing with the AG. First, the ECJ found that Articles 1 and 2 of the 1995 Directive provides that data processing systems must simultaneously respect fundamental rights and freedoms of privacy, and contribute to individual well-being, while ensuring the free flow of data; national laws on the processing of personal data should facilitate this balance.\textsuperscript{27} Second, Article 12(b) of the 1995 Directive provides that the data controller must facilitate “as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data.”\textsuperscript{28} Third, Article 14(a) provides that the data subject has a right to object to the data controller’s actions based on “compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data.”\textsuperscript{29}

This case pivoted on the interpretation of “data processing,” a legal question so important that several governments weighed in. With respect to the 1995 Directive’s application to search engines like Google, Mr. Costeja, the European Commission, and the Austrian, Italian, Polish,
and Spanish governments all maintained that search engines do engage in “data processing” under the 1995 Directive, and are therefore “data controllers.”\textsuperscript{30} Google denied that Article 2(b) should be applicable to its actions and the Greek Government maintained that search engines are only intermediaries and are not “controllers” unless they “store data in an ‘intermediate memory’ or ‘cache memory’ for a period which exceeds that which is technically necessary.”\textsuperscript{31} The ECJ ultimately determined that a search-engine operator is a data “controller” under the definition of 2(d), which is any “natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” even though the search engine does not exercise control over the personal data and only provides a decisive role in disseminating the data on the Internet, and significantly impacts the right to privacy.\textsuperscript{32}

Article 2(b) also defines “processing of personal data” as “any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.”\textsuperscript{33} The ECJ affirmed that loading personal data on the Internet meets the definition of “processing” under 2(b), and that a search engine in fact “collects,” “retrieves,” “records” and “organises,” “stores” on servers, and “discloses” and “makes available.”\textsuperscript{34}

With respect to the territorial scope of the 1995 Directive, the search engine “controller,” Google Inc., is a huge multinational corporation with global reach. But its Spanish subsidiary, which operates the Spanish version “www.google.es,” has a separate legal personality and has been located in Madrid since 2003. Google locates and sweeps up web-page content throughout the world, and collects revenues for advertising associated with a web user’s search terms (including in Spain), while Google Inc. has a local “establishment” in Spain for purposes of meeting Article 4(1)(a) of the 1995 Directive.\textsuperscript{35} Google, Inc. argued that even if there is a local “establishment,” the activities of the controller are not “carried out in the context of the activities” in Spain because Google Inc. runs the searches without Google Spain’s intervention, but Article 4(1)(a) does not require that the data be processed by the “establishment,” which is unnecessary when the search engine’s parent operations and the local establishment are “inextricably linked.”\textsuperscript{36}

\textsuperscript{30} Id. at ¶ 23.
\textsuperscript{31} Id. at ¶¶ 22, 24.
\textsuperscript{32} Id. at ¶¶ 32–36, 38.
\textsuperscript{33} Id. at ¶ 25.
\textsuperscript{34} Id. at ¶¶ 26, 28 (citing Case C-101/01, Lindqvist, 2002 E.C.R. I-12992, at ¶ 25).
\textsuperscript{35} Id. at ¶¶ 42–49.
\textsuperscript{36} Id. at ¶¶ 50–56.
On the question of Google's responsibility to respond to removal requests based on the person's name from third-party websites, including when the original publication is lawful, Google Spain and Google Inc. maintained that requests to remove information must be addressed to the website's publisher because that is where the ultimate responsibility resides, and because that party is the one that must defend its fundamental right to publish. But the ECJ pointed out that supervisory authority under Article 1 of the 1995 Directive is required to offer a high level of privacy protection and other fundamental rights and freedoms and Article 12(b) guarantees that Member States rectify or erase incomplete or inaccurate data that does not comply with the 1995 Directive.

Moreover, Article 6 requires the controller to ensure that "personal data are processed 'fairly and lawfully,'" consistent with and relevant to the legitimate purposes of collection and to keep the data accurate and up-to-date. Member States must give the data subject the right to object on legitimate grounds under Articles 7 and 14 of the 1995 Directive, and the data subject can make this request directly to the data controller, who must "duly examine" the merits of the objection. If the data controller does not grant the relief, the data subject can petition the "supervisory authority or the judicial authority," which may order the "controller to take specific measures accordingly," including by using "investigative powers and effective powers of intervention enabling it to order ... blocking, erasure of data or impose a temporary or definitive ban on such processing," including when the original publication of the information is lawful.

The ECJ pointed out that the data controller's economic interest in processing of personal data, as well as the general public's interest in finding information, can be "overridden by the interests or fundamental rights and freedoms of the data subject," which are invoked by retrieval of information by the subject's name. In making this decision, the supervisory authority or judicial authority must balance competing interests in the information against the privacy rights at stake, but it is also important to note that there may be a distinction in the rights of the data subject vis-à-vis the search engine but not against the publisher of the web page. The latter may have heightened rights, particularly when there is some specific journalistic purpose. Likewise, this balancing of rights is also found in Articles 7 (respect for privacy) and 8 (protection of

37. Id. at ¶ 62.
38. Id. at ¶ 63.
39. Id. at ¶¶ 66, 70.
40. Id. at ¶ 72.
41. Id. at ¶¶ 76–77.
42. Id. at ¶¶ 77–78, 88.
43. Id. at ¶¶ 74, 97.
44. Id. at ¶ 82.
45. Id. at ¶¶ 85–86.
personal data and effects and to rectify data) of the Charter of Fundamental Rights of the European Union ("EU Charter").

Consequently, the Google Spain case effectively placed "control" of the data in the "public authority," "agency," or "natural or legal person" under the 1995 Directive. "Natural or legal persons" now specifically includes search engines, requires more responsibility, and implicates a public obligation to uphold fundamental rights as specified under EU directives regarding privacy and other EU Charter rules. In this sense, the case also signals the possibility of an increasing obligation within the private sector to not only be subject to EU Directives but also to act as the initial screening device on behalf of Member State regulations.

There remain several controversial points deriving from the Google Spain case. First, the ECJ pointed out that when a search engine processes personal data, there is a fundamental right of privacy implicated; vast amounts of a person's private life can be revealed in a name search, but without the search engine, all of the detail and the interconnection among detail would only be available with great difficulty. Second, the data subject’s privacy rights are balanced against the search-engine user’s right to have access to information, but the disposition of that balance should depend on the specific case and the importance of the information to the public against the sensitivity of the data to the subject’s privacy. In effect, the ECJ provided a broader construction of the definition of "control" over personal data, which, in effect, can potentially shift deeper responsibility to additional Internet intermediaries for privacy violations. This, in turn, leads to the problem of privatizing regulation—allowing a private company to decide what that balance should be instead of a government body.

A third controversial outcome of this case concerns de-coupling regulatory control over companies like Google from a fixed physical processing location: "Google had argued that its operations in Spain amounted to not much more than a sales office, and therefore decisions over data protection from the EU did not apply—as all the data-crunching was done in the US." The ECJ disagreed. After the Google Spain case was handed down, Viviane Reding, the EU’s Commissioner for Justice, Fundamental Rights, and Citizenship, enthusiastically noted that American firms "can no longer hide behind their servers being based in California or anywhere else in the world. No matter where the

46. Id. at ¶ 69.
47. 1995 Directive, supra note 9, at 31, 38.
48. Google Spain, supra note 2, at ¶ 80.
49. Id. at ¶ 81.
51. In U.S. law, that would trigger a discussion of whether the function being delegated by the government to the private sector was indeed a "delegable" function.
physical server of a company processing data is located, non-European companies, when offering services to European consumers, must apply European rule."\(^{53}\)

This broader construction of “control” arguably allows the protection of both the free-expression rights of the source as well as the privacy rights of the searched subject. In other words, by not requiring *La Vanguarda* to alter the actual pages containing the content of which Mr. Costeja complained, the original source’s free-expression right (freedom of the press in this case) is ensured even though *La Vanguarda* clearly has the most “control” over the content. Google, which has less actual control over the content, but clearly more control over who sees it, is merely an intermediary between the searcher and the disseminator of the data in question and, as such, does not possess the same free-expression interest. Yet both the original publisher and the intermediary affect the rights of privacy, as the ECJ stated:

[i]nasmuch as the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights of privacy and to the protection of personal data, the operator of the search engine as the person determining the purposes and means of that activity must ensure, within the framework of its responsibilities, powers and capabilities, that the activity meets the requirements of Directive 95/46 in order that the guarantees laid down by the directive may have full effect and that effective and complete protection of data subjects, in particular of their right to privacy, may actually be achieved.\(^{54}\)

On the ECJ’s final inquiry, there was debate over how broadly the data subject’s right should be interpreted. For the last question, Google Spain, Google Inc., the governments of Greece, Austria, Poland, and the EU Commission argued that data subjects should only have a right to be forgotten if the data processing in question is incompatible with Article 12(b) and Article 14(a) of the 1995 Directive on compelling legitimate grounds, not just because the data subject wants information to sink into oblivion.\(^{55}\) Alternatively, Mr. Costeja and the Spanish and Italian governments argued there should be a right to be forgotten for the data subject that overrides “the legitimate interests of the operator of the search engine and the general interest in freedom of information.”\(^{56}\) The latter interpretation is more accurate in principle because Article 12(b) read in conjunction with 6(1)(c) to (e) of the 1995 Directive can apply to erase data that is accurate but still “inadequate, irrelevant or excessive in relation to the purpose of the processing, . . . are not kept up to date, or . . .

---

53. *Id.*
54. *Google Spain, supra* note 2, at ¶ 38.
55. *Id.* at ¶¶ 89–90.
56. *Id.* at ¶ 91.
are kept for longer than is necessary unless . . . required to be kept for historical, statistical or scientific purposes."\(^{57}\)

This decision, cementing the right to be forgotten in EU jurisprudence, will have an impact on a wide range of actors, including:

1. Users seeking information, pursuant to a right to receive such information;
2. The originator or publisher of information, generally publishing on the web based on freedom-of-speech rights;
3. The government, or regulators, making rules that impact any of the parties or overseeing the process;
4. Intermediate Internet services that permit data to traverse the web between publisher and users; and
5. The data subject that may have information retrieved from a search.

Internet intermediaries (companies) and data subjects (individuals) are particularly affected by government policy decisions. While the practice in the United States and elsewhere has been to provide immunity to intermediaries like Google, Google Spain created a policy fissure when search engines directly impact the rights of data subjects and derivatively impact whether government should be involved. A broad right to be forgotten can potentially reduce an Internet user’s ability to attain or more easily access their individual search results, all in the name of the search target’s rights. The more the rights of the data subject are promoted, the greater the impact on the search engine. With respect to individual companies, search-engine market share in January 2015 shows that the most significant impact is, unsurprisingly, on Google. The company holds 75.2% of the market share based on the number of searches (79.3% in January 2014) while Yahoo’s share is 10.4% (7.0% in January 2014).\(^{58}\) Google’s current market share of the search market in Europe is 90%.\(^{59}\) As of September 2014, Google granted about half of the 120,000 erasure requests it received.\(^{60}\)

The ECJ decision has redrawn the legal obligations of search engines like Google with respect to whether it “controls” data. Kent Walker, Google’s general counsel, stated that “[w]e like to think of ourselves

---

57. Id. at §§ 92, 94.
58. Robert Hof, Why Google’s Search Market Share Loss to Yahoo Means Pretty Much Nothing, FORBES (Jan. 8, 2015, 6:02 PM), http://www.forbes.com/sites/roberthof/2015/01/08/why-googles-search-market-share-loss-to-yahoo-means-pretty-much-nothing; see also W. Gregory Voss, After Google Spain and Charlie Hebdo: The Continuing Evolution of European Union Data Privacy Law in a Time of Change, 71 BUS. LAWYER 281, 281 (2015) (“[While] Google may seem to have been singled out in a year when that firm is also under European competition scrutiny, the lessons to be drawn [from the Google Spain case] are more broadly applicable.”).
as the newsstand, or a card catalogue... We don’t create the information. We make it accessible. A decision like this [from the ECJ], which makes us decide what goes inside the card catalogue, forces us into a role we don’t want.”

This opinion was reiterated by a National Post article, which offered the analogy of a man walking into a library and asking a librarian to remove all references in the library’s card catalog to a book containing information about the man because he is now a changed man and the information is irrelevant; the library, however, maintains that it cannot fulfill the request because this would make the library a censorship body.

Marc Rotenberg, president of the Electronic Privacy Information Center, challenged this analogy: “Google is no longer the card catalogue. It is the library—and it’s the bookstore and the newsstand. They have all collapsed into Google’s realm.” The library-card-catalog search may not be a precisely accurate analogy since a traditional library search often retrieves books that have a broader spectrum of knowledge as well as post-date-of-publication works that challenge the accuracy of the volume searched. Traditional publication processes also contain screening devices through layers of editing and peer review that help ensure accuracy. Alternatively, electronic news sources, websites, blogs, and other Internet sources can instantaneously spring up without the underlying support of screening from editors and publishing houses. Additionally, books are often not published specifically with the goal of being defamatory, unless nefarious acts about the subject are true. And if there are some controversial items in a book about a subject or person, it probably is not highlighted in the way that a Google search would retrieve the items. Unless it appears in electronic form or on Google Books, a book would need to be inspected to physically find the controversial information, but a search engine can take web users instantaneously to the precise location of the information in question.

Other specialists in the field support the notion that search engines like Google should be characterized as data controllers. Chris Scott, a partner at Schillings, remarked that it is reasonable for Google to be classified as a data controller because “Google does not merely passively deliver information; Google sculpts the results.” Steve Wood, Head of Policy Delivery at the British Information Commissioner’s Office, agreed, noting that Google is not a “mere conduit” with “information just passing through it,” but instead is much more involved in data use “[g]iven the level of interaction a search engine has and the interest it

61. Id.
63. Toobin, supra note 60.
64. EUROPEAN UNION COMM., supra note 4, at ¶ 27.
takes using algorithms when it is interacting with personal information and spidering the [I]nternet." 65

Once a legal regime like the right to be forgotten is created, forcing compliance by the private sector, the question of remedies for noncompliance must be addressed. In this case, the legal remedy can be injunctive and/or monetary in nature. For example, if the law develops in such a way that privacy is more fully protected *vis-à-vis* freedom of speech and Google does not reasonably comply with private or court requests to purge, the question is whether a data controller could then be sued for damages if there are adverse professional or personal losses as a result of a breach of reasonable conduct. Damages for failure to comply with a supervisory authority's order are severe: €1,000,000 or up to 2% of global turnover.66

From a regulatory standpoint, the existing EU approach originated with the 1995 Directive. To enforce the 1995 Directive, Article 22 provides that Member States can provide administrative remedies for aggrieved data subjects prior to the mandated authorities, with the mandated remedial steps including the creation of a supervisory authority and also a judicial authority so that “[m]ember States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question.”67 Article 28 lays out the mandate for a supervisory authority: “[e]ach Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive.”68

The supervisory authority shall:

1. Assist its particular Member State’s in drawing up “administrative measure[s] or regulations to the protection of individuals’ rights and freedoms with regard to the processing of personal data”;
2. Have investigative powers, such as to access the data at issue and collect necessary information;
3. Have intervention powers which include “delivering opinions before processing operations are carried out[,]... ordering the blocking, erasure or destruction of data, of imposing a temporary or definitive ban on processing, of warning or admonishing the

65. *Id.* at ¶ 28.
67. 1995 Directive, supra note 9, at 31, art. 22.
68. *Id.* at art. 28(1).
controller, or that of referring the matter to national parliaments or other political institutions"; and

4. Have “the power to engage in legal proceedings where the national provisions adopted pursuant to this Directive have been violated or to bring these violations to the attention of the judicial authorities.”

In effect, “independent” search-engine operators, as data controllers, “act under the supervision of national data protection authorities,” and national courts have the final say to address the balance between data protection and freedom of expression. For example, in the Google Spain case, it was the Spanish Data Protection Agency, Spain’s national authority for enforcing the EU directive, that was the implicated state authority when Mr. Costejo sought to have stories about him in La Vanguardia erased from Google search results.

The main policy critique leveled at the EU’s embrace of the right to be forgotten in the wake of Google Spain focuses on the shift in regulatory responsibility (balancing privacy and speech) from the government to the corporation, and the attendant danger of suppressing free speech—only a small step removed from censorship. The European Commission counters that the intention is to allow citizens to defend their own interests; furthermore, the right “does not allow government to decide what can and cannot be online or what should or should not be read.”

A related concern is that the way the ECJ decision was drafted effectively privatized regulation of important rights. It places too much autonomy and authority on privately-owned search engines to perform what might in other contexts be considered governmental policy and regulatory functions of oversight of data management and freedom-of-expression rights. On this latter point, Jules Polonetsky of the Future of Privacy Forum pointed out that the ECJ decision took what can be scenarios with complicated questions of fact and “require[s] Google to be a court of philosopher kings,” which “shows a real lack of understanding about how this will play out in reality.”

Requests to purge listings could become so numerous that Google may not be able to adequately respond on an individual evaluative basis, but rather may have to act by automatically withdrawing links en masse. The conservative corporate response would be to over-erase out of an abundance of caution to remain in compliance with the law and thereby avoid stiff penalties. Consequently, access to content with what may be

69. Id. at art. 28(3).
70. European Comm’n, Myth-Busting, supra note 5, at 5.
71. Google Spain, supra note 2, at ¶ 2.
72. European Commission, Myth-Busting, supra note 5, at 5.
73. See infra Part V.
74. Toobin, supra note 60.
75. EUROPEAN UNION COMM., supra note 4, at 15.
legitimate speech could be blocked without reasonably respecting the rights of the speaker simply because the private-sector official with the power to erase chooses to favor the petitioner. The choice to favor a petitioner’s right to erasure may be hyper-vigilant, but as there are no similar damages to be wary of with respect to infringement of free-speech rights, the corporate choice would be clear. Part III tracks Google’s compliance efforts in this regard.

III. COMPLIANCE EFFORTS UNDER THE NEW EU REGIME

Because the ECJ decision was against Google and because Google has some 90% of the search market in Europe,76 we look now at how Google has addressed complying with the new regime. Google’s current system seems to avert the danger of unreasonable erasure requests noted above. The ECJ decision was clear on what the right is and how it might arise, but it did not provide much in the way of guidance on how “controllers,” such as Google, could comply with the ruling. According to one legal commentator, Google complies by employing dozens of lawyers and paralegals to pore over the requests and adopting standards that include whether the petitioner is a private or public figure, whether the link is from a reputable news source or a government, whether the data subject actually published the information, and whether information consists of political speech or criminal charges.77 But in the absence of guidance from the ECJ, how did Google get there?

Google’s institutional response to the new requirements was to create an Advisory Council to Google on the Right to Be Forgotten (“Advisory Council”) in 2014. Convened by the chairman of Google and his general counsel, the Advisory Council’s charge was to design Google’s corporate response to the right to be forgotten.78

After meeting throughout the autumn and winter of 2014, the Advisory Council issued its Report in January 2015. The central question in the Report, around which all the policy recommendations are made, was this: “Google asked us to advise it on performing the balancing act between an individual’s right to privacy and the public’s interest in access to information.”79

76. Fairless, supra note 59.
77. Toobin, supra note 60.
78. The members of the council included: Luciano Floridi, Professor of Philosophy and Ethics of Information at the University of Oxford; Sylvie Kauffmann, Editorial Director, Le Monde; Lidia Kolucka-Zuk, Director of the Trust for Civil Society in Central and Eastern Europe; Frank La Rue, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression; Sabine Leutheusser-Schnarrenberger, former Federal Minister of Justice in Germany; José-Luis Piñar, Professor of Law at Universidad CEU and former Director of the Spanish Data Protection Agency (“AEPD”); Peggy Valkè, Professor of Law at University of Leuven; and Jimmy Wales, Founder and Chair Emeritus, Board of Trustees, Wikimedia Foundation. See LUCIANO FLORIDI, ET AL., REPORT OF THE ADVISORY COUNCIL TO GOOGLE ON THE RIGHT TO BE FORGOTTEN (Feb. 2015), https://buermeyer.de/wp/wp-content/uploads/2012/02/Report-of-the-Advisory-Committee-to-Google-on-the-Right-to-be-Forgotten.pdf.
79. Id. at 1. An extract from the Report may be found in Appendix A.
THE RIGHT TO BE FORGOTTEN

A. Implementation Criteria

The delisting criteria identified by the Advisory Council are grouped into four broad categories: (1) the data subject's role in public life (i.e., whether the person who is the subject of a delisting request is a recognizable figure or serves in public office); (2) the nature of information which is the subject of the delisting request (i.e., whether the information is of an intimate, financial, or other "sensitive" nature (in terms of the 1995 Directive, e.g.)); (3) the source of the information requested to be delisted; and (4) the timing (relevance) of when the information was posted.80

While the Advisory Council clearly made an effort to provide a comprehensive framework against which Google could establish workable parameters for evaluating removal requests, the question of whether the correct balance between privacy interests and free speech has been struck will remain unanswered until there is sufficient data to determine effect.

Nonetheless, it is possible to conceive of examples of censorship in the case of the search-engine intermediary not properly balancing the privacy right versus the freedom of speech. In one recent controversial decision of Google's erasure system, Robert Peston, the BBC's economics editor, wrote a blog post about Stanley O'Neal, the former CEO of Merrill Lynch, and Google deleted links to the blog post based on a request that came from a third-party.81 Or, if years have passed and a former government official, who may in fact be a war criminal, has not been convicted because of a fluke or technicality in the political or legal process that avoids objectivity from being applied in similarly situated cases, there could be an assumption that the facts surrounding those charges should be erased.82

B. Implementation Results

What have been the results in the first year of this policy implementation? Google released a report on November 23, 2015,83 showing which websites contained the most material triggering URL removal requests, how many requests were received, and how many were granted:

The new data shows that search results for Facebook are the most popular target for "right to be forgotten" requests, and that other sites in the top ten include YouTube and Twitter. The second most popular target for such requests is a "people search" site that

80. See id.
81. Toobin, supra note 60.
82. Id. (stating that "[t]he risk, according to the [New York] Times and others, is that aggrieved individuals should use the decision to hide or suppress information of public importance, including links about elected officials").
creates profiles of individuals by scraping data from social media sites.

The Google report also provides some hard numbers about just how many people are invoking the “right to be forgotten,” which took on legal force early this year when a European court said citizens could demand that Google scrub information that is “irrelevant” or “inadequate.”

Since then, the requests have been pouring in. According to the new Google data, the company has received 347,533 separate requests seeking to remove about 1.2 million websites. Google complied in 42% of the cases, meaning that over half a million results have disappeared from the European versions of its search engines.84

Consequently, the overall results demonstrate that Google is declining to grant the majority of requests for removal, with 58% being denied.85 Moreover, the chart below shows that both overall and by each country, the majority of removal requests (by percentage) are denied. That said, variations by country within the European Union are interesting and, in some cases, surprising. The following figures represent requests made versus requests granted by country between May 2014 and November 2015:

<table>
<thead>
<tr>
<th>E.U. Country</th>
<th>Total Removal Requests</th>
<th>% URL’s Removed</th>
<th>% URL’s Not Removed</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>247,823</td>
<td>48.4%</td>
<td>51.6%</td>
</tr>
<tr>
<td>Germany</td>
<td>222,319</td>
<td>48.2%</td>
<td>51.8%</td>
</tr>
<tr>
<td>U.K.</td>
<td>163,205</td>
<td>38%</td>
<td>62%</td>
</tr>
<tr>
<td>Spain</td>
<td>104,240</td>
<td>37.2%</td>
<td>62.8%</td>
</tr>
<tr>
<td>Italy</td>
<td>86,002</td>
<td>29.7%</td>
<td>70.3%</td>
</tr>
<tr>
<td>Austria</td>
<td>23,274</td>
<td>47.7%</td>
<td>52.3%</td>
</tr>
<tr>
<td>Belgium</td>
<td>37,472</td>
<td>45.7%</td>
<td>54.3%</td>
</tr>
<tr>
<td>Bulgaria</td>
<td>5,529</td>
<td>22.3%</td>
<td>77.7%</td>
</tr>
<tr>
<td>Croatia</td>
<td>11,482</td>
<td>31.7%</td>
<td>68.3%</td>
</tr>
<tr>
<td>Cyprus</td>
<td>1,042</td>
<td>44%</td>
<td>56%</td>
</tr>
<tr>
<td>Czech Rep.</td>
<td>16,401</td>
<td>44.2%</td>
<td>55.8%</td>
</tr>
<tr>
<td>Denmark</td>
<td>11,622</td>
<td>43.9%</td>
<td>56.1%</td>
</tr>
<tr>
<td>Estonia</td>
<td>8,325</td>
<td>43.1%</td>
<td>56.9%</td>
</tr>
<tr>
<td>Finland</td>
<td>16,591</td>
<td>43.3%</td>
<td>56.7%</td>
</tr>
</tbody>
</table>

85. Id.
86. See GOOGLE TRANSPARENCY REP., supra note 83. The number requests in column two reflect to the total number of requests made by “individuals with relationships to this country,” and not the actual number of requests originating from that country (a much smaller number), nor does this number correlate with the percentages of requests “processed” in columns three and four, which reflect “total evaluated.”
While French and German removal-request grant and denial rates generally track the overall rate (50-60% denied), Spain, Italy, and the United Kingdom stand out among the Western European states. The Spanish numbers are ironic, to be sure, given the Spanish case that anchored the right to be forgotten into the EU’s legal firmament. The British numbers are, however, interesting given the overwhelming British opposition to this EU right. Clearly, Google is granting more removal requests in France and Germany than elsewhere in Europe, and an especially few requests in the Balkans. Of course, there are other outliers like Malta, as well.

Extrapolation from such early published results may yield inaccurate conclusions. Some numbers may be skewed by date and/or level of URL-removal-request system implementation and public-education strategy by Google in each country. One may presume, however, from the tracking of requests, bifurcation between requests originating in that country (not represented on this chart) and only connected with that country, and disparity between requests and denials, that Google is actually undertaking serious evaluation of removal requests.

In its Transparency Report, Google provided some examples of its evaluative criteria at work in specific cases. In a British removal request, Google states that “[a]fter we removed a news story about a minor crime, the newspaper published a story about the removal action. The Information Commissioner’s Office ordered us to remove the second story
from search results for the individual’s name. We removed the page from search results for the individual’s name.”

Another British removal request resulted in partial removal:
A doctor requested we remove more than 50 links to newspaper articles about a botched procedure. Three pages that contained personal information about the doctor but did not mention the procedure have been removed from search results for his name. The rest of the links to reports on the incident remain in search results.

And in a third British example, Google states that “[a] man asked that we remove a link to a news summary of a local magistrate’s decisions that included the man’s guilty verdict. Under the UK Rehabilitation of Offenders Act, this conviction has been spent. We have removed the page from search results for his name.”

Several conclusions may be drawn from these instances of removal-request evaluation by Google. First, Google is apparently taking into account local national laws when considering these requests and applying them to the extent possible. Second, Google is demonstrating a level of detail in its review process that is demonstrative of actual individualized (not automated) review— a single request that contains multiple links can result in some of the links being erased while others are not. Third, Google will comply with local national regulatory-agency orders, when applicable, as it implements this policy. Whether this is indicative of institutional cooperation between Google and local-information government agencies or merely compliance is unclear.

C. Implementation Territorial Effect

A secondary issue concerning the implementation of the right is the scope of requests for URL removal. Google and its Advisory Council agreed that the removals should only extend so far as the databases in Europe. Council member Luciano Floridi, the Oxford professor, noted that “[g]lobal de-listing remains too controversial without an international agreement.” Moreover, Google maintained that 95% of searches were originating in the individual EU member states through local versions of Google (e.g., Google.uk for Britain or Google.de for Germany); thus, local implementation made more sense.

The EU, however, contends that the erasures should be global. Specifically, the EU’s Article 29 Data Protection Working Party, established by the 1995 Directive as an advisory group, maintains in an official guidance issued after the ECJ’s ruling in Google Spain:

87. GOOGLE TRANSPARENCY REP., supra note 83.
88. Id.
89. Id.
90. See Floridi et al, supra note 78, at 21–22.
92. Id.
Territorial effect of a de-listing decision: In order to give full effect to the data subject's rights as defined in the Court's ruling, de-listing decisions must be implemented in such a way that they guarantee the effective and complete protection of data subjects' rights and that EU law cannot be circumvented. In that sense, limiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.93

The EU Commission adopted the Article 29 Working Party's guideline, thereby extending court-mandated removal actions globally via administrative fiat.94 This puts Google in the position of updating its compliance efforts to meet what amounts to changing requirements on the part of the EU. Both validity and legitimacy arguments could be raised here—validity of administrative extension of judicial decisions without legislative processes, and legitimacy from a policy perspective.

At the national level, the French government's information commission, Commission Nationale de l'Informatique et des Libertés ("CNIL"), became the first national regulatory agency to require Google to extend its removals globally in June 2015 when it ordered Google to remove links from both the national domain (Google.fr) and the global database (Google.com).95 Free-speech advocates wasted no time criticizing CNIL's action as an overreach and a new manifestation of censorship.96

Google resisted the French legal mandate on policy grounds, stating that "no one country should have the authority to control what content someone in a second country can access."97 Google maintains that by requiring Google to go beyond delisting French removal requests on Google.fr and to also delist them on Google.com, France is unilaterally trying to determine what people in Japan or Brazil or elsewhere can see. Moreover, "Google warned that applying the right to be forgotten globally would trigger a 'race to the bottom' where 'the Internet would only be as free as the world's least free place.'"98

---

97. Google Refuses, supra note 91.
98. Id.
American First Amendment experts agreed with Google. Speaking with the New York Times, Harvard digital-law scholar Jonathan L. Zittrain noted that "'France is asking for Google to do something here in the United States that if the U.S. government asked for, it would be against the First Amendment[.]'" If the French regulator’s order were promulgated, Zittrain continued, Americans using an American search engine would be blocked from seeing content that is legal in the United States—"[t]hat is extremely worrisome to me." Google filed an appeal with CNIL in July 2015. CNIL considered Google’s appeal, but in September 2015 reaffirmed its decision. Legally, Google cannot appeal CNIL’s final decision. What Google can do is refuse to comply, thereby drawing penalties and fines that it can then appeal to the Conseil d’État (the French Supreme Court). The risk for Google in such a legal strategy could be very expensive. CNIL will likely begin to apply sanctions including the possibility of a fine in the region of 300,000 against Google, should the company refuse to comply with the order. Under incoming European regulation the fine could increase to between 2% and 5% of global operating costs.

While Google is engaged in legal struggles at the Member State level, it is likely that Brussels will move to implement its new draft Regulation in such a manner as to pre-empt further resistance from Google and other search engines. The current timeline for EU action on this front anticipates adoption and implementation of the Regulation in 2017.

IV. OTHER NATIONAL ANTECEDENTS AND ANALOGIES

The right to be forgotten was not plucked out of thin air by the ECJ in 2014. Nor was it wholly contained within the directives that gave rise to it. The right to be forgotten is a modern incarnation of sometimes well-worn theories in Western legal traditions. That said, there is wide variability among states. Privacy protections are “embarrassingly difficult to define,” “[are] an unusually slippery concept,” and “differ strangely from society to society.”

Dangers of data misuse can reach thresholds for unacceptability across different countries at different points. If one views different types of information on a continuum, there are different levels of perceived dangers to the rights of individuals based on the infringement and context. The ability to control the data becomes more difficult. In 2007, David J. Solove cited the danger inherent in living in a world where false,
defamatory, dubious, or even true but humiliating records on people can be preserved indefinitely and be quickly retrieved with a Google search, which results in an infliction being placed on the data subject who may find attaining a second chance, employment positions, or full freedom more difficult because of computer records. This can particularly be the case for ex-convicts who may have difficulty finding a job. Professor Viktor Mayer-Schönberger remarked that there can be an information overload that can confuse human decision-making even though forgetting in some cases may be preferable, and this trend of information overload may become even more profound as a consequence of the cost of digital storage dropping further. Public perceptions regarding a particular individual could be broadly and unreasonably distorted.

This section traces some of those privacy theories and applications to provide better intellectual and historical context to the current formulation.

A. In Continental Europe

The jurisprudential basis of a “right to be forgotten,” as derived from notions of a right to privacy or personal integrity, has a solid history in Europe. As Yale law professor James Whitman, a comparative-privacy-rights expert, notes:

[privacy is deeply connected with the protection of personal honor in Europe. Europeans focus on the impact the public distribution of embarrassing facts could have on personal honor or prestige; American privacy law lacks an equivalent orientation.]

107

The famous case of Alexandre Dumas illustrates this long-rooted preference for privacy rights over other competing rights. In 1867, the famous Three Musketeers author, then sixty-five-years old, posed for photographs, still a fairly new technology, with a very young American actress clad only in her underwear and presumed to be his mistress. Upon publication of the photos a scandal ensued; Dumas went to court to get the photos back. The French courts ultimately ruled that Dumas’ “right to privacy” superseded the photographer’s property rights...”

108

Dumas’ cause suffered a defeat in the lower court, which actually sided with the photographer. While settled French law maintained that with respect to portraiture, one owned the right to one’s image, and “portraitists in any medium could not publish the work without permission of the sitter”—in the Dumas case, the author had not paid for the
photographs and therefore could not assert superior property rights to those of the photographer. On appeal, the higher court reversed in favor of the author. Departing from the lower court’s focus on competing property rights, the higher court rested on the combined theories that “even if the distinguished author originally gave consent, he had the right to withdraw it; and that ‘on the grounds of public decorum, the cartes de visite are not such as ought to be sold.’” A contemporary notice of the case appeared in the British Journal of Photography:

M. Dumas and the Photographer—The Imperial Court of France has given the following judgment in the appeal of M. Alexandre Dumas against the photographer, Liébert: ‘Whereas, if it is customary for well-known persons who sit to photographers to grant the right of selling copies of their likenesses, that sale ought to cease from the moment that the person who has tacitly authorised [sic] it desires it to cease; whereas also this concession cannot be definitive and perpetual, and as to establish such an arrangement a private convention would have to be produced, which has not been done in the course of the trial; considering likewise that if private life ought to be protected in the interests of individuals, it ought to be equally so in that of morals and public decency; the Court rejects the appeal, but gives Liébert the benefit of an offer made to him by Dumas of an indemnity for his outlay, and fixes the sum at 100f., after the payment of which such, Liébert is prohibited from selling the resemblance in question and is required to deliver up the photographs to Dumas.”

The conflation of privacy interests and property interests, and the right to one’s own image, are various strands of legal theory that intertwined a century and a half ago and still do today. In 2015, Dumas would be requesting Google to delink his “digital” image, not just seeking a physical return of the scurrilous photographs. Moreover, the offending digital image can be one of words, as in the case of Mr. Costeja, or a literal image, as in the case of Mr. Dumas. In that sense, perhaps the right to be forgotten is merely a new sobriquet for a much older entrenched right that is much more pervasive in the civil-law world than the common law.

Many also trace the right to be forgotten’s legal origins in France (droit à l’oubli) and Italy (diritto al’oblio) as springing from the “right to oblivion”—defined as a right to silence over past instances that are no

111. Id.
longer transpiring. Under French law, the concept of a limitation on information is incorporated into both civil and criminal law, with the duration of forgetting depending on the subject matter, such as by category of offenses in criminal law. France takes the privacy of criminal records seriously and endeavors to rehabilitate former convicts. In the U.S. this analogously takes the form of expungement proceedings with respect to minor crimes.

Likewise, the French doctrine of droit moral incorporates the importance of moral rights and permits authors to keep, hold, and withdraw published work and a right to preserve the integrity of a published work. Other jurisdictions have codified similar rights tracing back to these early historical antecedents. There was no equivalent to the French concept of droit moral in U.S. law until the Visual Rights Act of 1990. Likewise, Spain and Germany have specifically incorporated a right to be forgotten into their law while Britain has not.

In some cases, "forgetting" can be encouraged to occur on a societal level instead of an individual level. When that happens, there is an opening for a culture of forgetting to set in that permeates that society. In Spain, the aftermath of the traumatic Franco dictatorship is a case in point. The origin of the phrase derecho al olvido in Spain relates specifically to the 1977 amnesty law that prohibited prosecution of those associated with the forty-year dictatorship of Francisco Franco, which followed a gruesome civil war that killed as many as 200,000 Spaniards. The amnesty law was adopted in order to move on with democracy, and was heavily backed by re-casted Francoists. The amnesty law has ostensibly impacted other societal institutions of knowledge in Spain. Spain’s Royal Academy of History does not use the word “dictator” in its encyclopedia entry on Franco, and history accounts have been sanitized with assuming that Franco’s forces were operating with reasonable force and “normalizing civilian life” when others would regard the accounts as brutalizing and “crimes against humanity.” So perhaps it is not all that surprising that the proliferation of recent “right to be forgotten” cases appeared in

118. Id. at 184.
119. Frantziou, supra note 50, at 774 n.93.
121. Id.
Spain, a society that is used to forgetting crimes committed during the Franco era.

More recently, in 2011, about ninety plaintiffs, with backgrounds as diverse as a prison guard, high-school principal, and plastic surgeon, petitioned Spain's Data Protection Agency, with the general political support of the Spanish government, to require Google to have specified Internet references with their names erased because accompanying information was embarrassing or unnecessary. This differs from cases in which requests are made to erase links due to either a potential copyright violation or defamatory or false content—a type of erasure request with stronger global support. The types of claims to a right to be forgotten raised in the run-up to the Google Spain case were based on a more flexible choice of basis by the petitioner and a lower threshold of tangible reason, legal infringement, and culpability by the originating webpage publisher.

Consequently, as cases arose, Google was placed in the middle of the free speech and privacy dispute and needed to work within a threshold of accommodating, rejecting, or burying links in its search results, but at the same time, not infringing free speech in a way that would make it appear to be willingly assuming a deeper role in controlling information flow. Yet, due to the global nature of the Internet and its ability to easily replicate information across jurisdictions, it was not possible to protect the subject's data by solely targeting the publisher of the web page, which may also assert freedom-of-speech rights. Consequently, Google appealed decisions that required the company to remove links and several cases were brought to Spain's National Court, including the Google Spain case which found its way to the ECJ.

In Italy, the right to be forgotten has taken on criminal dimensions. In 2010, Judge Oscar Magi imposed a six-month prison sentence on three Google executives for violating the privacy of a disabled boy in 2006 by permitting a video of the boy being teased and bullied by classmates to be posted on the Google Video site. Because it was only a six-month sentence, however, and Italy does not request extradition for sentences of less than three years, the sentences were suspended. Nonetheless, the sentences were challenged and reversed by the Court of Appeals in Milan. The Court of Cassation, Italy's Supreme Court, affirmed the

---

123. Blitzer, supra note 120.
124. Giles, supra note 122.
125. Google Spain, supra note 2, at ¶¶ 84-85.
126. Giles, supra note 122.
128. Id.
appellate ruling, finding that Google’s YouTube was merely a host provider that stored content posted by the users and determining that Internet services providers did not in fact have an affirmative obligation to monitor data provided by third parties.\textsuperscript{130}

Developments independent of the 2014 ECJ decision on the right to be forgotten occurred in Germany as well. The German Constitutional Court attempted to strike a balance between expression and privacy interests, with a landmark decision supporting privacy interests in the case of protection against secret tape recordings as long ago as 1973.\textsuperscript{131} The recent reliance by German courts on this “precedent” in the case of the Internet emerged in 2009. In 1990, Wolfgang Werl6 and Mafred Lauber were convicted of killing a German actor that same year.\textsuperscript{132} Because German law permits courts to suppress the name of convicted criminals from news accounts after the convicted individuals have paid their debt to society, as a right to privacy and policy of re-socialization, Werl6 and Lauber sued Wikipedia in German courts to expunge their names from Internet web pages.\textsuperscript{133} While removal from the German language versions of websites were not legally problematic, the English version of the Wikipedia listing posed more problems because the account was within the protection of the First Amendment in the U.S.\textsuperscript{134}

\textbf{B. In Latin America}

In Latin America, Argentina has been the most active in dealing with the right to be forgotten. The main case on record there arose before the \textit{Google Spain} case and is worth noting if only to observe another court in a different civil-law setting wrestling with the same issue, but using a different approach. Unlike Europe, Argentina has not specifically enacted legislation on the issue of search-engine liability. Consequently, Argentinian case law involves balancing competing rights instead of resolving the issue by classifying a search engine like Google as a data controller. The \textit{Da Cunha} case was the first highly public decision in Argentina on whether search engines were required to block or filter material in searches or face liability.\textsuperscript{135} In 2009, Virginia Da Cunha, an Argentine pop star, brought suit for 200,000 Argentine pesos against Google Inc. and Yahoo De Argentina S.R.L. for material and moral damages and to

\begin{itemize}
\item \textsuperscript{130} Bogdan, \textit{Italian Supreme Court: Google’s Youtube is Just a Hosting Provider}, EDRI (Feb. 12, 2014), https://edri.org/italian-supreme-court-search-engines-just-hosting-providers/.
\item \textsuperscript{131} Edward J. Eberle, \textit{Human Dignity, Privacy, and Personality in German and American Constitutional Law}, 1997 UT A H L. REV. 963, 970 n.20, 980 n.93 (1997) (citing Tape Recording Case, 34 BVerfGE 238, 245–51 (1973)).
\item \textsuperscript{133} \textit{Id.}
\item \textsuperscript{134} \textit{Id.}
\end{itemize}
enjoin the unlawful and unauthorized use of her image and name as it was associated with sexual, erotic, and sex trafficking websites.136

Judge Simari found in favor of Da Cunha,137 but recognized the opposing rights in question, which included Article 14 of the Argentine Constitution, guaranteeing the right to publish ideas without previous censorship; Article 32, prohibiting the Federal Congress from restricting freedom of the press; and general principles of liberty of thought and expression regardless of the medium of conveyance.138 The court, however, referenced the importance of the right to personal integrity and arbitrary/abusive interference in private life under international law, and derivative protection through the National Constitution, by anchoring this right as reflected in Article 5 of the American Declaration of the Rights and Duties of the Man, Article 12 of the Universal Declaration of Human Rights, Article 11.2 of the Pact of San Jose, and Article 17 of the International Covenant on Civil and Political Rights.139 The trial court also pointed out that Argentine civil law protects personal rights associated with publication and reproduction without one’s consent, and stated that the Argentine Supreme Court recognizes the right to image and the right to honor as separate rights.140

The case, however, was reversed on appeal in 2010.141 Petitioners maintained that there was a misestimate of material damages, and the general rules with respect to civil responsibility were not properly applied to search engines, particularly because there could be censorship and a requirement for search engines to react even though they do not have control over the web pages in question.142

According to one of the judges, Judge Patricia Barbieri, who voted to reverse, there was no specific legal norm that dictated an answer for this cause of action in Argentina; however, decree 1279/97 declares that Internet services are protected by Articles 14, 32, and 42 of the National Constitution, which prohibits prior censorship.143 Moreover, Law 26,032/05 provides that searching for and receipt of information on the Internet are protected forms of freedom of expression, and freedom of expression is guaranteed in Article 13 of the American Convention on

---

137. Id. at 16–17.
138. Id. at 11.
139. Id.
140. Id. (“[E]l derecho a la imagen es autónomo del derecho al honor o al decoro. Tal autonomía lo es también respecto del right of privacy o intimidad, para hacer ocupar al derecho a la imagen un puesto más alto en la escala de los valores humanos íntimamente conectados con la personalidad. El derecho a la imagen tiene un ámbito tutelar propio y autónomo, independiente de la protección de la intimidad o del honor.”).
142. Id. § V (Los agravios).
143. Id. § VI.
Human Rights. On the other hand, conflicting rights include those found in Article 1071 of the Civil Code, Article 31 of law 11,723 of Intellectual Property, and Article 19 of the Magna Carta, which provide for personal privacy and the right to image and likeness. Prior cases protected freedom of expression as a bulwark of democratic society, but those rights were not absolute. Instead, they were subject to rights to remedies for injuries to one's likeness, reputation, and honor, and these have been affirmed as rights in the media, press, and social media. In these cases, factors such as dissemination of the image without consent and privacy and honor rights could come into play.

Judge Barbieri noted that, despite competing rights, to extrapolate this form of liability was more complex in the case of the Internet because there is a publisher, an Internet-site owner, the Internet-service supplier, the computer operator seeking information, and the transporter of the interconnection across the diverse networks. With respect to the case at issue, no liability was apt to pass on to the supplier of Internet access. Consequently, it was unnecessary to consider the Internet-host-service providers and the role of search-program mechanisms that react to requests of the computer operator as it is individuals who control the content of websites (that are retrieved and referenced by the search engine) and who make decisions about content.

Judge Ana María R. Brilla de Serrat agreed with Barbieri, noting that there had been pertinent cases on the "right to be forgotten" issue in Italian courts for fifteen years, specifically with respect to whether confessed criminals who served their sentence should have their honor and reputation damaged by repeated publication in the news. The technolog-
logical reality, however, is that digital information may not disappear and is subject to cheap storage in computers, whereas throughout human history there is a propensity to forget more distant data and information.\textsuperscript{151}

Dissenting, Judge Diego C. Sanchez explained that the two opposing judges were overlooking the more straightforward means of factual and legal analysis and procedure.\textsuperscript{152} Judge Sanchez believed that the logistics of the retrieval of information was most important. He cited to William Blackstone's \textit{Commentaries on the Laws of England}, emphasizing that while it is true that a free press is equivalent to having a free State, that does not mean that there is a right to publish what is "improper, malicious, or illegal," and if one does so publish, the publisher must assume the responsibility for that recklessness.\textsuperscript{153}

Sanchez cited the 1984 Argentine Supreme Court case \textit{Ponzetti de Balbin} for the proposition that the exercise of "freedom of expression . . . does not authorize ignorance of the right of integral privacy as an essential freedom promised by the Constitution."\textsuperscript{154} He reasoned that computer-operated search-engine processes (such as the automated search and retrieval of text and images that fulfill the search criteria) should not separate the holder of the search program from the consequences and damages of operation just because it makes the program simpler and more convenient.\textsuperscript{155} To do otherwise, Judge Sanchez argued, would render Internet use impotent.\textsuperscript{156}

Judge Sanchez emphasized similarities in well-established law restricting the unauthorized use of one's image or likeness for commercial purposes, pointing out that those same property rights apply on the Internet.\textsuperscript{157} Moreover, Da Cunha did not grant consent to the use of the images, which should entitle her to damages.\textsuperscript{158} Meanwhile, Yahoo and Google were not to be considered neophytes at what they do, but in fact were known globally for their importance to Internet transactions and services to society (for profit), and Google's own terms of service already

\begin{itemize}
\item \textsuperscript{151} \textit{Id.}
\item \textsuperscript{152} \textit{Id.} § I (Sanchez, J. dissenting).
\item \textsuperscript{153} \textit{Id.} § III. Judge Sanchez noted in response to Google's allegation that there would be censorship, there was a distinction in free speech between prior restraint and subsequent responsibility; but even so, there are restrictions of the former type in the case of inappropriate material for children and child pornography. \textit{Id.} He went on to note that while it is true that Articles 14, 32, 42, and 75 of the National Constitution and Article 13 of the Pact of San Jose declare that "all persons have the right to liberty of thought and expression" and this right is included in Decree 1279/97 for the Internet, Article 11 of the American Convention on Human Rights also guarantees one the right to be free from "illegal attacks to his or her honor or reputation." \textit{Id.}
\item \textsuperscript{154} \textit{Id.} (quote translated from Spanish into English by authors).
\item \textsuperscript{155} \textit{Id.} Judge Sanchez also referenced Judge Guillermo A. Borda, who stated that the search-engine operations that facilitate retrieval of contents are framed in freedom-of-information and free-expression terms, but the operation is more like the antecedent of a consequent effect because there is a supplier of content, including potentially illegal content, that causes the damages, but the search engines make retrieval of the illicit material possible for economic gain. \textit{Id.}
\item \textsuperscript{156} \textit{Id.}
\item \textsuperscript{157} \textit{Id.} § IV.
\item \textsuperscript{158} \textit{Id.}
\end{itemize}
acknowledged an obligation to respond to copyright infractions. Moreover, general principles of liability exist that require a supplier of a good or service to respond to prevent further damage after being warned.

C. In North America

At about the same time that Alexandre Dumas was arguing his case before the French courts, "privacy" was also becoming a hot legal topic in the United States. For example, law partners Louis Brandeis and Samuel Warren wrote in their seminal article on the common-law tradition's right to privacy:

[i]njury of feelings may indeed be taken account of in ascertaining the amount of damages when attending what is recognized as a legal injury; but our system, unlike the Roman law, does not afford a remedy even for mental suffering which results from mere contumely and insult, from an intentional and unwarranted violation of the 'honor' of another.

While U.S. courts have been reluctant to force removal of information that offends personal rights, there are examples of public policy curbing the free flow of information at either the original source or secondary dissemination stage. One dramatic example is the case of eighteen-year-old Nikki Catsouras, who was in a fatal car accident in 2006. Photos of her partially decapitated body still in the car at the crash site taken by the California Highway Patrol ("CHP") were gruesome. Her body was in a condition such that the police would not permit Nikki's parents to identify it. Two weeks after the accident, the family learned that photos of the accident were circulating the Internet and being posted on thousands of websites because two CHP employees shared the photos with friends. This prompted the distraught family to take legal action to remove the photos from more than 2,000 websites, but even that did not fully prevent the circulation.

The Catsouras family undertook tort litigation to pursue a similar remedy—erasing photos of their daughter's corpse from the Internet. The U.S. does not have federal data-protection standards that rely on characterizing who is a "data controller" to impose such liability, but that is not to say that remedies are not available. Catsouras was a case of viral social media. Here, the concern is the liability of search engines to take down old, misleading, private, or irrelevant material. The United States does not have the same construct as Europe now does (imposing liability

159. Id. § V.
160. Id.
162. Toobin, supra note 60.
163. Id.
164. Id.
165. Id.
166. Toobin, supra note 60.
on an entity based on that entity's classification as a 'data controller'). Moreover, the privacy traditions are different. Yet, there are examples, albeit not completely analogous, where take-down requests have been made, but based on different legal routes—namely tort and civil litigation.

There is some consistency between the precedent of gag orders in the U.S. and the right to be forgotten in that the former involves a public interest in not naming names of perpetrators or victims in certain types of crimes and to protect witnesses. The difference is that this is a public policy that starts at the point of the event in question. The right to be forgotten has similar policy intentions, but even if there is not an overriding public interest at the time the event takes place, there may be a time lag that reduces the importance of the initial information. While U.S. precedent indicates that there can be an overriding privacy interest that prevails over freedom of speech at the time of original publication, this is the exception, not the rule. The trend has been to favor freedom of speech.

In an 8–0 opinion, the U.S. Supreme Court decided in Smith v. Daily Mail Pub. Co. (1979) that a West Virginia statute criminalizing the publication of the name of a juvenile charged with a crime without the authorization from the juvenile court was a violation of the First and Fourteenth Amendments. In this case, a fourteen-year-old student at Hayes Junior High School in St. Albans, West Virginia, shot and killed a fifteen-year-old student. The Charleston Daily Mail and the Charleston Gazette published the name of the alleged assailant after asking witnesses, the police, and an assistant prosecuting attorney on the day after the attack. Three different radio stations also published the names of the assailant on the day of the attack.

The West Virginia statute stated that "nor shall the name of any child, in connection with any proceedings under this chapter, be published in any newspaper without a written order of the court..." and punished the offender of the proscribed publication with a misdemeanor offense. Consequently, the state interest in protecting the privacy interest of the juvenile offender was overridden by the First Amendment right to publish lawfully-obtained and truthful information because the prior restraint on speech can only be punished when it is necessary to further the asserted state interests. In this case, the statute failed to accomplish its stated purpose of protecting the anonymity of the juvenile because it only restricted newspapers, but not electronic media.
More broadly speaking, there are public-policy reasons for restricting the freedom of information with respect to court records. Nevertheless, there are exceptions, such as the privacy interests of assault victims. In *Cox Broadcasting Corp. v. Cohn* (1975), the victim of a gang rape was killed by the attackers, and the victim's father brought a civil suit against *Cox Broadcasting* for revealing his daughter's name. The Supreme Court ruled that the First and Fourteenth Amendments prevail over the interests of privacy for information that is already part of the public record. And in the case of *Florida Star v. B.J.F.* (1989), in violation of a Florida statute, the *Florida Star* published the name of a sexual-assault victim prior to trial, but liability was not imposed on the *Florida Star* because the Supreme Court ruled that when there is information of public interest that is lawfully obtained by the newspaper, dissemination cannot be constitutionally punished. In this case, it was the sheriff's department that failed to keep the information private under the Florida statute.

In the United States today, while victims and suspects of most types of violent crimes are quickly and routinely publicly disclosed, treatment of victims of sexual assault raise additional concerns and protections, which has led many news organizations to voluntarily adopt policies prohibiting the disclosure of the identity of sexual-assault victims. Additionally, some state statutes prohibit news organizations from disclosing rape-victim identities, at least prior to trial. For example, in *M.G. v. Time Warner, Inc.* (2001), the court held that minors and coaches had a right to privacy in the case of *Sports Illustrated* and HBO's *Real Sports* publishing a story that involved reports of coaches molesting the players on a little-league team.

The Supreme Court has not broadly decided either to always protect privacy or always protect the First Amendment without restriction in the case of publicizing the identity of a victim of sexual assault. Congress also has not articulated an overarching position one way or the other, but it has shown it can act decisively in certain instances. In 1994, it passed the Violence Against Women Act, which created a federal restriction on the subject entity's disclosure of confidential information of "victims of domestic violence, dating violence, sexual assault, or stalking" without express permission. The underlying policy rationale was to ensure that

---

176. Id. at 496.
179. *ENCYCLOPEDIA OF AMERICAN CIVIL LIBERTIES* 1261 (Paul Finkelman, ed. 2006).
“news media, law enforcement officers, and other persons should exercise restraint and respect a rape victim’s privacy by not disclosing the victim’s identity to the general public or facilitating such disclosure without the consent of the victim.”

V. THE BRITISH RESPONSE

A. Pre-Brexit Response

Shortly after the ECJ handed down its decision in the Google Spain case, cementing the right to be forgotten into European jurisprudence, the British House of Lords conducted an inquiry, collected evidence, and issued a report in July 2014 recommending that the British government not incorporate this right. The House of Lords European Union Committee’s Subcommittee on Home Affairs, Health, and Education acknowledged that

the degree to which modern technology has eroded the privacy of data subjects. Once information is lawfully in the public domain it is impossible to compel its removal, and very little can be done to prevent it spreading. Where there is information about individuals which they would prefer not to be widely known, they are wholly reliant on those who know the information not to make it public, or to publicise it further.

They disagreed, however, with the EU’s incorporation of a right to be forgotten to resolve this problem. Government, academic, and private-sector witnesses all endorsed this view with respect to the ECJ decision implementing the current EU Directive, but also with respect to the EU’s new draft Directive. Indeed, on the latter point, the British Information Commissioner’s Office asserted its continuing antipathy toward a right to be forgotten:

[t]he UK would not want what is currently in the draft [EU Directive], which is the right to be forgotten, to remain as part of that proposal. We want it to be removed. We think it is the wrong position. I do not think, both as an individual and a Minister, we want the law to develop in the way that is implied by this judgment, which is that you close down access to information in the EU that is open in the rest of the world.

[T]he Government does not support the right to be forgotten as it is currently proposed by the European Commission . . . . It is currently in their draft; we oppose that and we have made that clear in the negotiation . . . we are not going to shift our view in negotiations that the right to be forgotten must go. We are very clear about that and we are going to argue the case both in terms of the wrongness of the principle—because we believe in freedom of infor-

183. EUROPEAN UNION COMM., supra note 4, at ¶ 5.
The House of Lords agreed with this position. Describing the EU’s right to be forgotten as “misguided in principle and unworkable in practice,” the Lords were persuaded that search engines such as Google should not be considered data controllers, and that generally “[i]t is no longer reasonable or even possible for the right to privacy to allow data subjects a right to remove links to data which are accurate and lawfully available.”

Furthermore, they found that unevenness in treatment among search engines and the specter of censorship should be avoided.

In our view the judgment is unworkable. It ignores the effect on smaller search engines which, unlike Google, may not have the resources to consider individually large numbers of requests for the deletion of links. It is wrong in principle to leave to search engines the task of deciding many thousands of individual cases against criteria as vague as ‘particular reasons, such as the role played by the data subject in public life.’ We emphasize again the likelihood that different search engines would come to different and conflicting conclusions on a request for deletion of links.

The British press was overwhelmingly in agreement with the House of Lords’ position. BBC News began leading with stories only a week after the ECJ decision with headlines like “Politician and Paedophile Ask Google to ‘Be Forgotten’” reporting that:

Google has received fresh takedown requests after a European court ruled that an individual could force it to remove “irrelevant and outdated” search results, the BBC has learned.

a. An ex-politician seeking re-election has asked to have links to an article about his behaviour in office removed.

b. A man convicted of possessing child abuse images has requested links to pages about his conviction to be wiped.

c. And a doctor wants negative reviews from patients removed from the results.

In an act of defiance against the right to be forgotten’s effect on UK free-press rights, British newspapers and online news providers began publishing lists of stories that had been taken down by Google. BBC News was on the vanguard of this effort as its Managing Editor, Neil McIntosh, personally took to the web to publish fixed links to articles

184. Id. at ¶ 52–53.
185. Id. at ¶ 61–62, 64.
186. Id. at ¶ 56.
previously searchable on BBC News via Google but which have since had their URLs removed.\footnote{188} In so doing, he noted that

[each month, we'll republish this list with new removals added at the top. We are doing this primarily as a contribution to public policy. We think it is important that those with an interest in the ‘right to be forgotten’ can ascertain which articles have been affected by the ruling. We hope it will contribute to the debate about this issue. We also think the integrity of the BBC’s online archive is important. . . . The pages affected by delinking may disappear from Google searches, but they do still exist on BBC Online.\footnote{189}]

A minority of opinions in British press circles went the other way. For instance, a contributing editor to the \textit{Guardian} criticized the BBC’s action (even though her own newspaper was following suit), noting that “the British press is an outlier in Europe. No other countries have been republishing requests.”\footnote{190} Nevertheless “various [other] publishers including the \textit{Telegraph}, the \textit{Guardian} and the \textit{Daily Mail} have published lists of the stories on their sites for which links were removed.”\footnote{191} Appendix B contains a list published by the \textit{Telegraph} of its newspaper articles that have been erased from Google’s search results. The authors have arranged these articles by type of information contained therein.

\section*{B. Post-Brexit Possibilities}

In a June 23, 2016 national referendum called by the Conservative government of Prime Minister David Cameron, the British public voted 52\% to 48\% in favor of leaving the European Union.\footnote{192} Mr. Cameron’s successor, Theresa May, will be tasked with triggering Article 50 in the Treaty of Lisbon which commences an exit negotiation process between London and Brussels that could take up to two years.\footnote{193} Depending on the outcome of the negotiations, Britain will presumably be free from the jurisdiction of the ECJ and no longer bound by the underlying case that requires implementation of the right to be forgotten in Britain. Any associated directives, regulations, or decisions would also presumably cease to have legal effect in the UK.

In that case, Britain could then go do a different direction and create a data regulatory environment that allows Google to carve out the Google.uk domain as an exception to this right—an action that would

\begin{thebibliography}{99}
\footnotesize
\bibitem{188} Neil McIntosh, \textit{List of BBC Web Pages Which Have Been Removed from Google’s Search Results}, BBC\textsc{internet Blog} (June 25, 2015, 14:40), http://www.bbc.co.uk/blogs/internet/entries/1d765aa8-600b-4f32-b110-d02fbf7fd379.
\bibitem{189} Id.
\bibitem{191} Michael Rundle, \textit{Read the BBC Stories Purged from Google over ‘Right to Be Forgotten,’} \textit{Wired} (June 25, 2015), http://www.wired.co.uk/article/bbc-right-to-be-forgotten.
\bibitem{192} Krishnadev Calamur et al., \textit{Britain, Post-Brexit,} \textit{Atlantic} (July 13, 2016), http://www.theatlantic.com/news/archive/2016/07/brexit-results/488561/.
\bibitem{193} Id.
\end{thebibliography}
likely be brought about via Parliamentary action. Alternatively, Google could seek a declaratory judgment post-Brexit establishing that “[w]hen Britain is out [of] the EU, Google can, if they want to, apply to a British court for a ruling that in the UK there is no right to be forgotten.”

British lawyers are struggling to figure out what the future of the right to be forgotten is in the UK. For example, according to the London tech firm Addleshaw Goddard,

at present, the right to be forgotten has been rolled out across Europe by Google and includes google.com (following the CJEU Case of Google v Gonzalez). After Brexit the CJEU decision may no longer apply to the UK and it is possible Google would be permitted to carve out all google.co.uk domains from this blanket shield and UK citizens will lose this right.195

Others point out that keeping the right to be forgotten might be the cost of doing business with the EU as part of a larger trade pact. According to law firm Taylor Wessing:

the fact is that, in many areas, if we do not comply with EU law, we will not be able to trade with the EU. Areas of law which are particularly unlikely to change include data protection . . . . [I]f we do not comply with EU legislation and take into account CJEU rulings on relevant legislation, we will significantly restrict our ability to trade with the EU. The reason this extends to CJEU rulings is because they interpret EU law. If we choose to keep a piece of EU-derived legislation or adopt a new piece, we will arguably need, from a practical perspective, to apply any CJEU decisions in respect of those laws. The recent high profile examples in the area of data protection in the Google Spain and Schrems decisions (which dealt respectively with the right to be forgotten online and data exports from the EU to the USA), illustrate how CJEU decisions can significantly affect non-EU Members.196

Thus, the right to be forgotten, like all other British law derived from EU law, could remain effective if the UK decides it is a necessary component of a larger data protection agreement with the EU—which will be part of the new bilateral trade negotiations. As Taylor Wessing also noted,

[i]t is hard to quantify exactly how much UK law has been adopted as a result of EU requirements; estimates of how much UK law was influenced by EU law between 1993–2014 vary from around 13% to 62%. What is certain is that we have a lot of EU-derived law already on the statute books and there are major questions as to

how this will be dealt with and how we will deal with new EU law
which we might be required to follow in order to continue trading
with the EU in certain areas, for example, in consumer sales of
goods, services and digital content. The answer to these questions
will depend partly on which exit route the UK takes.197

VI. FREE SPEECH: A CONSTITUTIONAL BUFFER?

Will the new European “right to be forgotten” cross the Atlantic
and come to North America? While privacy rights are protected in the
United States and Canada as well, the answer really centers on whether
the American and Canadian versions of free speech are comparatively
stronger than privacy.

Constitutionally speaking, many think that they are. According to
Wikipedia founder Jimmy Wales, who also served on Google’s Advisory
Council, the Google Spain case laid bare a cultural gap that had already
existed for quite some time between Europe and the U.S. over privacy
rights and free speech.198 As documented in an interview with the BBC’s
technology correspondent

Wales, who divides his time between London and the US, ex-
plains . . . why something like [the right to be forgotten] could never
happen across the Atlantic because of the constitutional guarantee
of free speech: “This is not a debate the United States is even capa-
able of entering into. You’d have to repeal the First Amendment—
and that’s like a religious artefact—so that’s never going to happen.”199

There is similar skepticism in Canada. Halifax lawyer David Fraser,
a partner with McInnis Cooper and privacy/Internet specialist, “doesn’t
believe this could be implemented in Canadian law, because the Charter
of Rights and Freedoms ‘has a guarantee of freedom of expression—we
don’t have a guarantee of your right to be forgotten.’”200 Fraser also notes
that “Europeans generally put a greater emphasis on privacy rights,
which can be seen in their attitudes to the online world.”201

Generally speaking, the preference for putting more legal weight
behind free-speech or privacy rights in modern Western democracies
tends to track whether the legal system of the society in question rests on
a common-law or civil-law tradition. Like Britain, Canada, and the U.S.
are traditionally common-law countries202 and, therefore, place more rel-

197. Id.
199. Id.
200. Andre Mayer, ‘Right to Be Forgotten:’ How Canada Could Adopt Similar Law for Online
Privacy, CNC NEWS (June 16, 2014), http://www.cbc.ca/news/technology/right-to-be-forgotten-how-
canada-could-adopt-similar-law-for-online-privacy-1.2676880.
201. Id.
202. These common-law countries do, however, contain societies with civil-law traditions like
Louisiana and Quebec.
ATIVE emphasis on freedom of speech than a right to privacy.\textsuperscript{203} The opposite is the case in continental European countries— which are all rooted in the civil-law tradition.

The fact is the EU is dominated by civil-law Member States, as is the ECJ—which is dominated by judges from civil-law traditions, and this helps explain the preference now placed on privacy rights (as articulated in the right to be forgotten) over competing free-speech rights—despite an official policy to balance the two. The recent enforcement action by France’s CNIL against Google,\textsuperscript{204} however, belies this gloss of balance by clearly preferring privacy over speech, and doing so in such a way as to infringe the free-expression rights of innocent third parties in distant countries outside France by forcing Google to extend its removal actions globally, not just in France.

There is an unavoidable conflict between the right to be forgotten and the right to know, the latter of which pertains to the rights of the recipient of the message and derives from the sender’s freedom of speech. The right to be forgotten is a type of privacy concern that is perhaps best conceptualized in accordance with what Americans might perceive as a combination of privacy\textsuperscript{205} and false light (or negative light),\textsuperscript{206} and is based on protecting one’s personal dignity.

There is debate over how these competing rights should be viewed. Professor Luciano Floridi, who served on Google’s Advisory Council, stated that it is best not to rank rights in a hierarchical order but instead, “one is better off saying that it depends on specific instances, contexts and practices, and there is no useful, general way of establishing \textit{a priori} what comes first and what comes later, but only intelligence and wise discernment.”\textsuperscript{207}

Implicit in the analysis of these specific rights is the nature of the information sought to be removed. At one end of the spectrum there is a consensus emerging that if posting certain information breaches criminal law, such as in the case of posting child pornography, the data controller must remove the link to it and search engines must act on these requests and must also remove links to copyright-infringing material.\textsuperscript{208} Something that would be found in the middle of the spectrum might include aged information about a less-serious criminal conviction while a more-serious recent conviction might more fully implicate a public right to know. Or, at the other end of the spectrum there could be information that a data subject would prefer to have removed even if it is not defamatory or does not involve clear civilly protected interests.

\textsuperscript{203} Mayer, supra note 200.

\textsuperscript{204} Gibbs, supra note 101.

\textsuperscript{205} See, e.g., Stanley v. Georgia, 394 U.S. 557, 568 (1969) (“[T]he States[’]... broad power to regulate obscenity ... simply does not extend to mere possession [of obscene materials] by the individual in the privacy of his own home.”).


\textsuperscript{207} EUROPEAN UNION COMM., \textit{supra} note 4, at ¶ 4 (internal quotations omitted).

\textsuperscript{208} \textit{Id.} at ¶ 8.
The extraterritorial reach that results from the ECJ decision, at least via the CNIL enforcement action, is an attempt to force implementation of the right outside Europe. But setting aside the impact question and focusing instead on whether the right to be forgotten could arrive in full force in North America, a brief comparative analysis of privacy rights in the U.S., Britain, and Canada is necessary. It is important to note how such rights are articulated in each legal system to understand the legal weight accorded them. Whether a right to privacy is written into a constitution on the same basis as a right to free speech goes to whether it is accorded similar, superior, or inferior legal weight.

In the United States, there is no general right to privacy embedded in the text of the U.S. Constitution; the general right to privacy is constructed via the judicial system. The U.S. Supreme Court found a constitutional privacy right to exist *inter alia* within the meaning of the Fourth Amendment. Thus, current U.S. privacy rights have less textual legitimacy than free-speech rights, which are accorded pride of place in the First Amendment in the Bill of Rights. Such construction is in contrast to the European concept of privacy and protection of personal information, which is safeguarded by Article 8 of the European Convention on Human Rights ("ECHR"), in part, affording "a right to respect for private and family life." Significant legal protection is applied to any information considered personal concerning a specific person. Entities wishing to circumvent European privacy rights may only do so within narrowly constructed laws ensuring citizens' notice of intrusion into their private information.

Thus, in the United States, when these rights collide, free speech usually wins. For example, freedom of speech will prevail even when the subject of the publication could be embarrassed by the publication, as long as the story is true. In the case of applying traditional notions of privacy and freedom of speech on the Internet, there is a question of whether it should not just be the webpage that is protected speech, but whether Google and Yahoo's search results should be considered protected speech. On the one hand there is the right to receive information on the Internet, and on the other there is the subject of the search, but for both sides there is the website source, which also has the right of free expression.

Expanding traditional U.S. constitutional Fourth Amendment privacy jurisprudence relating to physical proximity to cyberspace and expanding obligations to an online intermediary would require overcoming

---

210. *Id.* at 294-95.
211. *Id.* at 269.
212. *Id.* at 260.
213. *Id.*
214. *Id.*
215. See *Florida Star v. B.J.F.*, 491 U.S. 524, 532 (1989) (holding that the imposition of damages on a newspaper for publishing the name of a rape victim violated the First Amendment).
some seemingly insurmountable hurdles erected by over two hundred years of First Amendment jurisprudence. By contrast, in Europe the ECHR came to recognize a fundamental protection of human rights not just against the state but against private individuals, corporations, and other organizations, resulting in a "positive obligation" of constitutional rights at the horizontal level such that "it becomes the duty of courts and other state agents to ensure that constitutional rights traditionally limiting only state action would also be enforced against private actors." Nonetheless, at the core of the debate are free-speech rights and privacy rights. Those rights may be weighed more fully either for the searcher or the data subject and the webpage or the search engine; however, the type of information and the age of the information would seem critical.

In addition to the constitutional analysis, there are legislative examples as well, predominately in the copyright context. In 1998 Congress passed the Digital Millennium Copyright Act ("DMCA"), which governs online distribution of text, photos, and video. DMCA contains a safe-harbor clause which absolves a service provider from liability for copyright-infringing works but requires that the work be removed with notice or when it is subject to an injunction.

Under § 512(c)(1)(A) of the DCMA, a service provider can attain a safe harbor protection only if it:

(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing; . . . (ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or . . . (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material.

Likewise, the safe harbor is available only if the service provider "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity."

Shielding websites from copyright-infringement liability helps ensure Internet freedom. That said, under a statutory argument protecting property rights, Google already complies with erasure requests. In a one-month period, Google may receive approximately thirty-one million requests to remove links in its search engine due to petitioner claims of copyright violation, and Google states that it accedes to the overwhelming majority of requests.

218. Id. § 512.
219. Id. § 512(c)(1)(A).
220. Id. § 512(c)(1)(B).
Another legislative example is the Communications Decency Act of 1996 ("CDA"), which was adopted to address child pornography, criminalizing perpetrators who send patently offensive, obscene, or indecent, sexual materials or comments to minors.222 In interpreting the CDA, the New York Supreme Court in *Stratton Oakmont, Inc. v. Prodigy Services Co.* imposed liability on the online service provider of a chat board, which posted guidelines for commentators, used screening software, and oversaw the guidelines for comments.223 The court determined that Prodigy was holding itself out by actively engaging in editorializing, and made service providers less likely to monitor comments provided by participants.224

Federal legislation, however, quickly sought to limit the liability under the CDA, which states: "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."225 The applicability of the "Good Samaritan" provision under § 230(c), however, provides that the interactive computer service will not be liable for "any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."226

To date, U.S. courts have shied away from imposing excessive legal obligations on online intermediaries for acting as a conduit and temporarily holding content. In applying these statutes, the trend in the courts is not to find that service providers are generally in control of third-party data (absent some specific activity covered by a statutory mandate).

The court in *A & M Records, Inc. v. Napster, Inc.* held that "if a computer system operator learns of specific infringing material available on his system and fails to purge such material from the system, the operator knows of and contributes to direct infringement."227 The court further held that unless there is "specific information which identifies infringing activity, a computer system operator cannot be held liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material."228

In *Viacom International Inc. v. YouTube, Inc.*, Viacom filed a $1 billion lawsuit against YouTube under the Copyright Act of 1976229 for illegally posting over 76,000 copyrighted videos in previous years.230 The

224. *Id.* at *4.
226. *Id.* § 230(c)(2).
228. *Id.*
court held that the service provider must become aware of specific unauthorized material in order to have a "power of authority" over an infringing item to thereby remove it.\footnote{In 2013, District Judge Louis L. Stanton dismissed the case, holding "YouTube did not have the right and ability to control infringing activity within the meaning of § 512 (c)(1)(B)."\footnote{Viacom Int’l Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 122 (S.D.N.Y. 2013).}} With respect to the claim of syndicating copyrighted material, the court held that "the critical feature of these transactions is not the identity of the party initiating them, but that they are steps by a service provider taken to make user-stored videos more readily accessible (without manual intervention) from its system to those using contemporary hardware," which provide protection under the § 512(c) safe-harbor provision.\footnote{Judge Howard Matz granted summary judgment in 2009 for Veoh because Veoh is protected under the DMCA against damage claims.\footnote{Id. at 1116-17.} On appeal, the court stated Veoh had a policy in place that endeavors to achieve compliance with the DMCA: Veoh had a notice and takedown procedure designed to ensure unauthorized material is quickly removed.\footnote{UMG Recordings, Inc. v. Veoh Networks Inc., 665 F.3d 1022, 1040 (9th Cir. 2013).}}

After filing the appeal, Viacom and Google, which acquired YouTube, settled the claim and Google announced "[t]his settlement reflects the growing collaborative dialog between our two companies on important opportunities, and we look forward to working more closely together."\footnote{Bradley McAllister, Google’s YouTube and Viacom Settle Copyright-Infringement Suit, JURIST (Mar. 18, 2014), http://jurist.org/paperchase/2014/03/google-and-viacom-settle-copyright-infringement-suit.php.}

In 2007, UMG sued Veoh—which provides web-sharing services similar to YouTube—for contributory and vicarious copyright infringement. Judge Howard Matz granted summary judgment in 2009 for Veoh because Veoh is protected under the DMCA against damage claims.\footnote{Id. at 1116-17.} On appeal, the court stated Veoh had a policy in place that endeavors to achieve compliance with the DMCA: Veoh had a notice and takedown procedure designed to ensure unauthorized material is quickly removed.\footnote{Id. at 1043.} Moreover, DMCA § 512(c) states that there must be "specific infringing activity the provider knows about" and the "general right and ability to remove materials from its services is, alone, insufficient," but "a service provider cannot willfully bury its head in the sand to avoid obtaining such specific knowledge."\footnote{"Viewing the evidence in the light most favorable to UMG, as we must here, we agree with the district court there is no evidence that Veoh acted in such a manner. Rather, the evidence demonstrates that Veoh promptly removed infringing material when it became aware of specific instances of infringement."} Both the appellate and district court agreed there was no evidence Veoh acted unreasonably in denying knowledge and not removing infringing material when knowledge was possessed.\footnote{UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1100 (C.D. Cal. 2009).} In 2013, the appellate court updated the 2011 opinion to be consistent with Viacom International Inc. v. YouTube, Inc., and specified that actual knowledge under § 512(c) is an objective standard whereas subjective "red flag" knowledge
of a specific infringement turns on "whether the provider was subjectively aware of facts that would have made the specific infringement 'objectively' obvious to a reasonable person."240

Both the Viacom v. YouTube and UMG v. Shelter Capital Partners (Veoh) cases stand for the proposition that active hosts have liability protection. The question of the level of knowledge required before some liability could attach, however, remains contested.

At the state level, there are some new developments arguably trending towards the establishment of right-to-be-forgotten legal foundations. California's SB 568, the "Privacy Rights for California Minors in the Digital World," which went into effect on January 1, 2015, gives minors who are registered users of an operator's Internet website the right "to remove or, if the operator prefers, to request and obtain removal of, content or information posted on the operator's Internet websites, online service, online application, or mobile application by the user" vis-à-vis the operator of a website when the operator has "actual knowledge" that the petitioning minor uses the site.241

Exceptions to this right include: (1) federal or state law requiring that the content be maintained, (2) the content was posted to the operator's Internet website by a registered user other than the minor, (3) the operator treats the content as anonymous so the registered user minor cannot be identified, (4) the minor does not correctly follow the operator's instructions on how to erase or delete the content, and (5) the minor received compensation for the content (but with some exceptions).242

This right to be forgotten is similar to the public policies consistent with permitting minors to annul contracts and a means of protecting people from previous indiscretions while a minor.

Specific to the question of erasing previously publicized records after the passage of time, in January 2015, the Second Circuit Court of Appeals decided Martin v. Hearst Corporation and upheld the U.S. District Court for the District of Connecticut's ruling against Plaintiff-Appellant Loraine Martin.243 Martin and her two sons were arrested in 2010 and local media outlets published print and Internet stories, including a statement that Martin had been "arrested and charged with numerous drug violations Aug. 20 after police received information that a pair of brothers were [sic] selling marijuana in town," which Martin acknowledges were true at the time of publication because police did find "marijuana, scales, plastic bags, and drug paraphernalia" after police conducted a search of her home.244

Connecticut's Criminal Records Erasure Statute, however, provides that criminal records of an arrest be destroyed if a person is found not

240. UMG Recordings, Inc., v. Shelter Capital Partners, 718 F.3d 1006, 1025 (9th Cir. 2011).
242. Id. at § 22581(b).
244. Id. at 548-49.
guilty, pardoned, or charges are nulled or dismissed, such that the person is assumed to have never been arrested for the offense in question. Martin later maintained that because the criminal case was nulled and the Erasure Statute was applicable in January 2011, failing to remove the accounts of her arrest on websites was false, defamatory, placed her in a false light before the public, negligently inflicted emotional distress, and invaded her privacy by appropriation because the Erasure Statute assumes the person was never arrested. The court acknowledged that the impact of a criminal arrest can be profound, long-lasting, and result in discrimination, including when someone is found not guilty of the charges, and the policy of undoing this stigma is the intention behind an erasure statute.

The court stated that the erasure statute creates a legal fiction that expunges the arrest itself for practical and legal effect for purposes of justice and law enforcement, but the legal fiction "does not and cannot undo historical facts or convert once-true facts into falsehoods." The Connecticut Superior Court "does not, and could not, purport to wipe from the public record the fact that certain historical events have taken place." Consequently, because there was truth to the newsworthy story at the point in time of the arrest, the tort-related claims related to the publication must fail. The court surmised that reasonable readers would know that charges are dropped against some percentage of those arrested, and publishers need not provide an update that the charges were nulled.

Consequently, while American courts and Congress are pulling at the threads of the big issues surrounding the right to be forgotten, they are still only pulling at threads. The full collision of competing rights of privacy and speech at the core of the right to be forgotten has not been addressed either in the legal or policy spheres in the United States to the extent it has in Europe. And, for now at least, free speech (and the associated right to know) would likely still prevail over competing privacy rights such as those which are the basis of the right to be forgotten.

Under British law, the process by which civil rights, including the right to privacy, are enforced is significantly different from the U.S. system. The United Kingdom does not have a written constitution. Free-speech rights have a much longer legal history, indeed a centuries-old

245. Id. at 549 & n.2 (citing CONN. GEN. STAT. § 54-142a(e)(1) (2015) (providing that “[a]ny person who shall have been the subject of such an erasure shall be deemed to have never been arrested within the meaning of the general statutes with respect to the proceedings so erased and may so swear under oath.”)).
246. Id. at 549.
247. Id. at 549–50.
248. Id. at 551.
250. Id. at 552.
251. Id. at 553.
252. James, supra note 209, at 285.
history, in Britain than do privacy rights. Notably, British rights afforded to British citizens are only semi-codified, with a few legal charters and Acts of Parliament creating a base of "'quasi-enforceable' civil and human rights that British citizens may assert against governmental encroachments."\textsuperscript{253}

Civil rights have only recently been outlined in the UK, achieved in part by modeling portions of UK domestic law, the Human Rights Act of 1998 ("HRA"), on the ECHR.\textsuperscript{254} "British citizens now enjoy most, but perhaps not all, of the 'rights' enumerated within the ECHR (e.g., the right to respect for privacy and family life, the right to free expression and assembly, the rights of due process and fair trial, the right to be free from discrimination, etc.)."\textsuperscript{255}

The rights provided by the HRA, however, are not impermeable.\textsuperscript{256} Furthermore, while it can be stated that the HRA is Britain's closest equivalent to the U.S. Bill of Rights, the latter enjoys a much more exalted legal status than the former because it is 'entrenched' within American domestic law and, as with the U.S. Constitution, it is considered to be legally sacrosanct.\textsuperscript{257} This is a matter of legal durability more than anything else. Statutes are more easily changed than constitutions. All it takes is a parliamentary majority. Although of vast significance, the HRA is legally analogous, technically, to any other statute that exists under domestic British law.\textsuperscript{258} "Therefore, taken in conjunction with the British doctrine of 'parliamentary sovereignty,' the HRA can be legislatively altered in the same fashion as any other Act of Parliament."\textsuperscript{259}

Once a right is lodged in the Constitution through the amendment process, it can only be removed or supplanted by amendment—an arduous process requiring agreement among 2/3 majorities of both houses of Congress and 3/4 of the states.\textsuperscript{260} While freedom of speech has been so lodged in the U.S., a general right of privacy has not—it was added by judicial interpretation. Thus, it can be equally removed by judicial re-interpretation. Comparatively, British rights to speech and privacy, encased in a statute, are both less protected from subsequent change (speech) and more protected (privacy) than in the U.S., where speech is fixed in the constitution and privacy can be changed by the judiciary. Separation-of-powers doctrine explains why.

In the U.S., the three branches of government, Executive, Legislative, and Judicial, are regarded as coequal. The Judiciary, charged with interpreting laws, has the authority to nullify laws or statutes incompati-

\textsuperscript{253.} Id. at 287.  
\textsuperscript{254.} Id.  
\textsuperscript{255.} Id.  
\textsuperscript{256.} Id. at 288.  
\textsuperscript{257.} Id. at 287–88.  
\textsuperscript{258.} Id. at 288.  
\textsuperscript{259.} Id.  
\textsuperscript{260.} U.S. CONST., art. V.
THE RIGHT TO BE FORGOTTEN

ble with the Constitution or the Bill of Rights. In contrast, British courts only retain the ability to declare statutes incompatible with the HRA, and by association, the ECHR. This lack of judicial review results in an acknowledgement of disharmony, but not invalidation or revision of language. 261 Statutes deemed incompatible with privacy provisions and protections of the HRA can therefore be enacted to the detriment of British citizens with very little judicial relief. "[I]t is worth noting, however, that under the HRA, British citizens enjoy a right of appeal to the ECHR, provided that the petitioner has first exhausted all of his or her domestic avenues of redress and appeal under UK law."

Within Canada, privacy rights are created and protected in part via the constitution and partly by statute or regulation. 263 The Canadian Constitution is actually an amalgamation of: (1) codified Acts of the British and Canadian Parliaments (e.g., the Constitution Act of 1867, the Constitution Act of 1982, the Canada Act of 1982 and the Canadian Charter of Rights and Freedoms; collectively enacted within Part I of the Constitution Act of 1982, etc.), (2) uncodified Canadian customs and (3) various other conventions, proclamations and pacts. 264

As such, Canada parallels the UK with a semi-codified constitution that is "technically 'written,' but the doctrines are not combined into a single written document." 265

For Canadians, the Canadian Charter of Rights and Freedoms mirrors a bill of rights. 266

As with its American counterpart, the Charter contains a number of fundamental civil rights and freedoms, such as: (1) freedom of conscience, thought, expression and belief, (2) the right to vote, (3) freedom of expression, free assembly and of the press, and (4) the right of life, liberty and security of the person. 267

As is the case with the U.S. Constitution, there is no express mention of privacy in the Canadian Charter; "however, the explicit rights to 'life, liberty and security of the person' and also 'freedom from unreasonable search and seizure' may be construed as a philosophical implication for such a right in Canada. " 268

Correspondingly, in 1983, the Canadian Parliament took it upon itself to enact the Privacy Act in order to vindicate a comprehensive right of privacy for Canadians. In relevant part, the Act regulates how the government may collect, store and eventually disseminate any Canadian citizen’s personal information. Further, the Act stipulates that individuals have a right of access to information held by

261. James, supra note 209, at 288.
262. Id.
263. Id. at 272.
264. Id.
265. Id.
266. Id. at 273.
267. Id.
268. Id.
the federal government and also the right to request correction of any erroneous information. In this respect, the Act is not remarkably different from the U.S. Privacy Act.269

Only applicable to federal government institutions, the Canadian Privacy Act “relates to an individual’s right to access and correct personal information the Government of Canada holds about them or the Government’s collection, use and disclosure of their personal information in the course of providing services (e.g., old age pensions or employment insurance).”270 However, as a federation, Canada is divided into provinces and territories; every province and territory has its own public-sector legislation, and relevant provincial acts will apply to provincial government agencies, not the Privacy Act.271

With respect to private actors posting data on the Internet without consent, Canadian law provides some tort remedies as a deterrent to such conduct, albeit in a categorized way. For example, in January 2016, a new law came into effect in Manitoba—the Intimate Image Protection Act.272 Taken in conjunction with the 2014 amendment to the federal criminal code adding the crime of “[publication] of an intimate image without consent,”273 an Ontario civil-court judge found that in the case of an unauthorized release of a woman’s sex video by her former boyfriend onto Internet pornography sites, “there are both established and developing legal grounds that support the proposition that the courts can and should provide civil recourse for individuals who suffer harm arising from this misconduct and should intervene to prevent its repetition.”274

The case went on to examine tort liability on the basis of several grounds, including breach of confidence, intentional infliction of mental distress, and invasion of privacy. The court then awarded the plaintiff damages of $105,500 plus costs and injunctive relief.275 Noting the dynamic of legal remedies catching up to new developments in technology, the Ontario judge said that

[i]n recent years, technology has enabled predators and bullies to victimize others by releasing their nude photos or intimate videos without consent. We now understand the devastating harm that can result from these acts, ranging from suicides by teenage victims to career-ending consequences when established persons are victimized. Society has been scrambling to catch up to this problem and the law is beginning to respond to protect victims.276

To summarize, wherever the right to speech or privacy may exist within the constitutional firmament of common-law societies, the general

269. Id.
271. Id.
272. C.C.S.M. c. 187, s. 11 (Jan. 15, 2016) (Can.).
274. Jane Doe 464533 v. D., 2016 ONSC 541, at ¶ 19 (Can.).
275. Id. at ¶ 69-70.
276. Id. at ¶ 16.
inclination to value speech over privacy tends to prevail. Because common-law societies place more power in their judicial systems, where judges are able to "make law," remedies like privacy-based tort actions are attractive because they do not suppress free expression before the fact—they only punish speakers after the fact if the law is broken. According to Daphne Keller, director of Intermediary Liability at Stanford Law School's Center for Internet & Society,

Europe's [right to be forgotten] laws are rooted in citizens' rights to data protection and privacy. They are inconsistent with U.S. and other countries' free expression laws, because they require suppression of information even if that information is true and not causing harm. In the U.S., the First Amendment would not allow a court to force a search engine to delist this kind of data.277

This common-law preference for speech over privacy, as generally reflected in U.S. law, may explain the British reaction to the EU's construction of the right to be forgotten emanating from the ECJ decision. It may also indicate that there is currently a constitutional buffer erected around North America which would make difficult the wholesale importation of the European version of the right to be forgotten. Where does this leave North America and Europe on either side of the Atlantic—to each his own? Maybe. As one popular cyber-journalist put it in a recent op-ed:

[c]ountries have to be able to apply their national laws online as they do offline—the two are intertwined now—but it cannot be the case that national or regional laws are pushed onto other countries as well. Both Europe and the U.S. believe in free speech and privacy, but Europe gives more weight to privacy and the U.S. sees free speech as non-negotiable. Neither should mess with the other's chosen balance of rights.

Americans are going to hit the roof over the suggestion that a European court can override their precious First Amendment, and I really cannot blame them. It's wrong.278

The broad trans-Atlantic disagreement on Internet-privacy rights remains. Whether multinational corporations that exist on both continents can comply with disparate regulations is another matter. And whether there is political will in the citizenry of both to register a clear preference for privacy or speech, or vice versa, in the context of the Internet is yet to be determined as well. Right now, these are judicial and administrative matters taken up in distant EU-level institutions, not expressions of parliaments or representative bodies.

VII. CONCLUSION

As the right to be forgotten gains traction and clarity through successive articulations, there will be winners and losers. More concrete economic implications will certainly follow. The battle as we know it has now commenced in Europe, but is set to expand globally, as policy, rights, and economic stakes become higher. Not surprisingly, interest groups and specialized firms are forming to engage on what the profile of the right to be forgotten looks like. Would Americans support the right to be forgotten here? In a recent poll, in September 2014, 61% of Americans favored some form of a right to be forgotten, 39% wanted a broad European-style right, and 47% believed that “irrelevant” search results can harm reputations.279

But public opinion is movable and interest groups are a potential mover. The question of interest groups funding the right to be forgotten cause can be viewed first as a reverberation on a political issue inside countries and secondarily as traditional advocacy-group initiatives. First, at the state level, there are underlying market considerations that may fuel tensions. On February 24, 2015, Günther Oettinger, the European Commissioner for Digital Economy, lashed out at Google Inc. and Facebook Inc. for exploiting legal loopholes that have permitted them to gather and sell the personal data of individuals.280 Oettinger further remarked that disputes over Google concern profitability for U.S. technology giants and stated that “[t]he Americans are in the lead, they’ve got the data, the business models and so the power. . . . [Google and Facebook] will go to the members states where data protection is least developed, come along with their electronic vacuum cleaner, take it to California and sell it for money.”281

This position came after a vote in November 2014 in which the European Parliament, for the first time, proposed breaking up a company and targeted Google’s bundling of services to its search business. European Parliament members Andreas Schwab and Ramon Tremosa stated that “[i]n case the proceedings against Google carry on without any satisfying decisions and the current anti-competitive behaviour continues to exist, a regulation of the dominant online web search should be envisaged.”282 Two U.S. government committees countered the claims and maintained that the EU is not committed to open markets because it is targeting U.S. companies, with Senators Ron Wyden and Orrin Hatch and Congressmen Dave Camo and Sander Levin stating that “[t]his and

280. Fairless, supra note 59.
281. Id. (internal quotations omitted).
similar proposals build walls rather than bridges [and] do not appear to
give full consideration to the negative effect such policies may have on
the broader U.S.-EU trade relationship.\textsuperscript{283}

Interest groups and attorneys are now beginning to specialize in
right to be forgotten claims. For example, the Electronic Frontier Foun-
dation ("EFF"), founded in 1990, has championed privacy issues and
freedom of expression through political activism and litigation and so-
cial-interest litigation.\textsuperscript{284} Given the EFF's recognition of the importance
of both privacy and freedom of speech, the EFF accentuated the im-
portance of implementation in the recent ECJ judgment by finding fault
not with the ECJ judgment, European privacy law, or Google's response,
but with "the impossibility of [applying] an accountable, transparent, and
effective censorship regime in the digital age, and [facing] the inevitable
collateral damage borne of any attempt to create one, even from the best
intentions."\textsuperscript{285} Other American consumer groups have supported, and are
advocating for some form of a right to be forgotten,\textsuperscript{286} but others also
point out the public interest in ensuring that a right does not go so far
because information needs to be accessible.\textsuperscript{287}

In Spain, interest groups such as the Association for the Recovery
of Historical Memory pressure the government to address past crimes
and atrocities. Such groups generally oppose the ECJ decision, with
Emilio Silva, president of the Historical Memory organization, remark-
ing that cleansing one's image sounds great, but Spain is a "factory of
forgetting."\textsuperscript{288}

In Argentina, attorneys have specialized in privacy issues relating to
the Internet and brought over two hundred claims on behalf of plaintiffs.
Argentine lawyer Adolfo Martín Peña was active in bringing cases
against Google and Yahoo to erase search results that would provide
links to content and photographs, with some originally being posted on
websites with permission and others without permission, the claims of
which are often directed at a name associated with websites that have
sexually suggestive content or involve pornography.\textsuperscript{289} Because Argentine
law did not clearly have an answer, new causes of action were driven
by lawyers who were specializing in those sorts of claims with plaintiffs who
wanted to impose more intense and proactive obligations on search en-
gines.

\textsuperscript{283} Id. (internal quotations omitted).
\textsuperscript{284} About EFF, ELEC. FRONTIER FOUND., https://www.eff.org/about.
\textsuperscript{285} Danny O'Brien & Jillian York, Rights That Are Being Forgotten: Google, the ECJ, and Free
Expression, ELEC. FRONTIER FOUND. (July 8, 2014), https://www.eff.org/deeplinks/2014/07/rights-are-
being-forgotten-google-ecj-and-free-expression.
\textsuperscript{286} Consumer Watchdog, supra note 279.
\textsuperscript{287} Julia Powles & Mario Costeja González, How Google Determined Our Right to be Forgotten,
GUARDIAN (UK) (Feb. 18, 2015, 02:30 PM), http://www.theguardian.com/technology/2015/feb/18/the-
right-be-forgotten-google-search.
\textsuperscript{288} Blitzer, supra note 120.
\textsuperscript{289} Carter, supra note 135, at 23-24.
So the conversation about the right to be forgotten is continuing, leaking out of the courtroom's chambers and Europe's borders. Internet-governance entities that currently exist on the international level are ill-equipped to deal with issues as profound as this. Nor should they. It is a job for states to undertake and come to agreement on in a broader sense. Europe has led the way on this issue. How many follow suit will be interesting to see. It could be that, in the end, perhaps "on the Internet, nobody knows you're a dog" after all.

VII. APPENDICES

APPENDIX A

Criteria for Assessing Delisting Requests

We identified four primary criteria on which we advise Google to evaluate delisting requests from individual data subjects. None of these four criteria is determinative on its own, and there is no strict hierarchy among them. Furthermore, social or technical changes may cause these criteria to evolve over time.

4.1. Data Subject's Role in Public Life

As explicitly noted in the Ruling, the role an individual plays in public life will weigh on the balancing act Google must perform between the data subject's data protection rights and the public's interest in access to information via a name-based search. The first step in evaluating a delisting request should be to determine the individual's role in public life. These categorizations are not in themselves determinative, and some evaluation along the other criteria laid out below is always necessary. However, the relative weight applied to the other criteria will be influenced by the role the individual plays in public life.

In general, individuals will fall into one of the following three categories:

- Individuals with **clear roles in public life** (for example, politicians, CEOs, celebrities, religious leaders, sports stars, performing artists): delisting requests from such individuals are less likely to justify delisting, since the public will generally have an overriding interest in finding information about them via a name-based search.

- Individuals with **no discernable role in public life**: delisting requests for such individuals are more likely to justify delisting.

- Individuals with a **limited or context-specific role in public life** (for example, school directors, some kinds of public employees, persons thrust into the public eye because of events beyond their control, or individuals who may play a public role within a specific community because of their profession): delisting requests from such individuals are neither
THE RIGHT TO BE FORGOTTEN

less nor more likely to justify delisting, as the specific content of the information being listed is probably going to weigh more heavily on the delisting decision.

Data subjects related to individuals playing a role in public life present some interesting edge cases, as they may themselves play a role in public life which can be significant. However, in similar cases, special attention should be paid to the content of the delisting request, as the data subject’s public role may be circumscribed. For example, there may be a strong public interest in information about nepotism in family hiring.

4.2. Nature of the Information

4.2.1. Types of information that bias toward an individual’s strong privacy interest

1. Information related to an individual’s intimate or sex life. In general, this information will hold increased weight of privacy rights in the balancing test against public interest. The exceptions will generally be for individuals who play a role in public life, where there is a public interest in accessing this information about the individual.

2. Personal financial information. Specific details such as bank account information are likely to be private and warrant delisting in most cases. More general information about wealth and income may be in the public interest. For example, in some countries, the salaries and properties of public employees are treated as public information; stock holdings in public companies may be of public interest; or there may be valid journalistic concerns in wealth and income information, including investigations of corruption.

3. Private contact or identification information. Information such as private phone numbers, addresses or similar contact information, government ID numbers, PINs, passwords, or credit card numbers will hold increased weight of privacy rights in the balancing test against public interest.

4. Information deemed sensitive under EU Data Protection law. Information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, health, or sex life may all have specific privacy protections in Europe. However, when such data relates to the role the data subject plays in public life, there can be a strong public interest in accessing links to this information via a name-based search.

5. Private information about minors. There is a special privacy consideration for children and adolescents according to the United Nations Convention on the Rights of the Child.

6. Information that is false, makes an inaccurate association or puts the data subject at risk of harm. False information or information that
puts the data subject at risk of harm, such as identify theft or stalking, weighs strongly in favor of delisting.

7. Information that may heighten the data subject's privacy interests because it appears in image or video form.

4.2.2. Types of information that bias toward a public interest

1. Information relevant to political discourse, citizen engagement, or governance. Political discourse is strongly in the public interest, including opinions and discussions of other people’s political beliefs, and should rarely be delisted.

2. Information relevant to religious or philosophical discourse. Religious and philosophical discourse is strongly in the public interest, including opinions and discussions of other people’s religious and philosophical beliefs, and should rarely be delisted.

3. Information that relates to public health and consumer protection. Information related to public health or consumer protection issues weighs strongly against removal. For example, reviews of professional services offered to the public at large may impact consumer safety; this value is widely recognized in the context of journalistic exceptions. Today, sources such as individual users on social media sites often provide this type of information, more so than traditional journalistic sources.

4. Information related to criminal activity. Data relating to offences or criminal convictions warrants special treatment under EU Data Protection Law. Where specific laws relating to the processing of such data provide clear guidance, these should prevail. Where none applies, the outcome will differ depending on context. The separate considerations of severity of the crime, the role played by the requestor in the criminal activity, the recency and the source of the information (both discussed below), as well as the degree of public interest in the information at issue will be particularly relevant in assessing these cases. The evaluation of the public interest in the delistings requested may differ depending on whether they concern a criminal offender or victim of a criminal offense. Information regarding human rights violations and crimes against humanity should weigh against delisting.

5. Information that contributes to a debate on a matter of general interest. The public will have an interest in accessing individual opinions and discussion of information that contributes to a public debate on a matter of general interest (for example, industrial disputes or fraudulent practice). The determination of a contribution to public debate may be informed by the source criterion, discussed below, but once information about a particular subject or event is deemed to contribute to a public debate there will be a bias against delisting any information about that subject, regardless of source.

6. Information that is factual and true. Factual and truthful information that puts no one at risk of harm will weigh against delisting.
7. Information integral to the historical record. Where content relates to a historical figure or historical events, the public has a particularly strong interest in accessing it online easily via a name-based search, and it will weigh against delisting. The strongest instances include links to information regarding crimes against humanity.

8. Information integral to scientific inquiry or artistic expression. In some cases, removing links from name-based search results will distort scientific inquiry; in those cases the information may carry public interest valence. The artistic significance of content constitutes public interest and will weigh against delisting. For example, if a data subject is portrayed in an artistic parody, it will weigh in favor of a public interest in the information.

4.3. Source

In assessing whether the public has a legitimate interest in links to information via a name-based search, it is relevant to consider the source of that information and the motivation for publishing it. For example, if the source is a journalistic entity operating under journalistic norms and best practices there will be a greater public interest in accessing the information published by that source via name-based searches. Government publications weigh in favor of a public interest in accessing the information via a name-based search.

Information published by recognized bloggers or individual authors of good reputation with substantial credibility and/or readership will weigh in favor of public interest. Information that is published by or with the consent of the data subject himself or herself will weigh against delisting. This is especially true in cases where the data subject can remove the information with relative ease directly from the original source webpage, for example by deleting his or her own post on a social network.

4.4. Time

The ruling refers to the notion that information may at one point be relevant but, as circumstances change, the relevance of that information may fade. This criterion carries heavier weight if the data subject’s role in public life is limited or has changed, but time may be a relevant criterion even when a data subject’s role in public life has not changed. There are types of information for which the time criterion may not be relevant to a delisting decision—for example information relating to issues of profound public importance, such as crimes against humanity.

This criterion will be particularly relevant for criminal issues. The severity of a crime and the time passed may together favor delisting, such as in the case of a minor crime committed many years in the past. It could also suggest an ongoing public interest in the information—for ex-
ample if a data subject has committed fraud and may potentially be in new positions of trust, or if a data subject has committed a crime of sexual violence and could possibly seek a job as a teacher or a profession of public trust that involves entering private homes.

Time may also weigh on determining the data subject’s role in public life. For example, a politician may leave public office and seek out a private life, or a CEO may step down from his or her role, but information about his or her time in that role may remain in the public interest as time goes on.

This criterion may also weigh toward approving delisting requests for information about the data subject’s childhood.  

APPENDIX B

List of TELEGRAPH (UK) newspaper articles that have been erased from Google’s search results

- A story about a British former convent girl who was jailed in France for running a ring of 600 call girls throughout Europe in 2003. Police were tipped-off about Margaret MacDonald’s operation by a former colleague following an argument.
- A second article, entitled *The Vice Queen of Windsor*, detailing MacDonald’s arrest and the allegations made against her, has also had its link removed.
- An article from 2008 about a former Harrow pupil, Alex Fiallos, who returned to his halls of residence after a night out drinking and drove his £4,000 car around the grounds at speeds of 30mph before crashing. He eventually collided with a set of steps in a scene reminiscent of the 1969 cult classic movie starring Michael Caine. His parents had given him the silver Mini just the day before.
- A story which includes a section taken from the rambling “war plan” of Anders Behring Breivik to massacre 100 people.
- A story from 2009 on our property page documenting how Paul and Fiona Godwin-Brown and their two boys Tom and Charlie gave up pressured London life and moved into a rolling Devon valley.
- A news story from 2003 on former president of the Law Society, Robert Sayer, being accused of inventing a phantom identity in order to have his former deputy expelled from the profession.
- Two stories from 2010 relating to football referee Dougie McDonald coming under scrutiny for a penalty decision in a Celtic v Dundee United match, and subsequently resigning. Both links were subsequently reinstated by Google.

290. Floridi et al., *supra* note 78, at 7–14 (citations omitted).
• Four images—which are actually two unique images, each hosted twice as separate copies on the Telegraph website—relating to Max Mosley’s 2008 sex scandal. (First image, second image)

• Two 2001 stories reporting that three men had appeared in court after being arrested when explosives were found in a Dublin apartment. The three men had been seen looking at something in a car, then refused to stop when police later attempted to pull them over. Inside the car were balaclavas and plastic boxes with switches attached to them, which “could be used as incendiary devices”. Follow-up searches of a number of homes found explosives and similar equipment to that found in the car.

• The link to an article from 2001 about a newspaper sales director who “terrorised” a shopkeeper and his wife in an incident before a football game was removed after Google received a request under the EU’s “right to be forgotten”. Patrick McVeigh, who was thirty at the time and earning more than £40,000 a year at Yorkshire Post newspapers, was heading for a football game at Leeds United with his brother Terence and a group of friends when he stopped to steal beer from a newsagent. His brother was also seen removing a security camera.

• An article from 2000 detailing the jailing of a butcher who threatened to send his estranged wife’s wealthy parents videos of her participating in group sex, which he filmed. Julian St Quinton was sentenced to two and a half years imprisonment for blackmail and nine months for indecent assault.

• A seventeen-year-old being issued with a three-year Asbo for being held responsible for almost 40% of the crime in a single town. Kyle Ivison, aged seventeen at the time, was held responsible for a crimewave of more than 120 offences in the town of Clitheroe, Lancs.

• Dr Edward Erin was jailed for six years in 2009 for attempting to spike his pregnant mistress’ drinks with drugs to cause her to miscarry their son. The link concerned was an article detailing an email Erin sent to a colleague following his arrest in February 2008.

• An article concerning a vicar who resigned after villagers accused him of standing naked at a vicarage window, swearing at children and staggering around drunkenly.

• A pensioner’s body lay undiscovered in her home in Norwich for up to six months before it was discovered by police in August 2011. Norfolk Coroner William Armstrong described the case as “deeply disturbing”.

• Tim Blackstone, a former porn star and brother of Baroness Blackstone, was found guilty of two counts of insider trading in 2003.

• An army captain who accused her commanding officer of labelling her a “blonde bimbo” had her claim dismissed by an employment tribunal in 2002.
Mark Wilson, a Scottish man, was jailed for life in 2002 for strangling his wife with a tartan tie and hiding her body under their bed for a week.

Two 2002 articles relating to the same story on how a Rolls-Royce driver ‘pulled a gun on Mayfair cabbie’ in 2002 and was subsequently jailed for four months.

A woman claimed gynaecologist Darwish Hasan Darwish raped her after putting her in a ‘deep hypnotic state’, causing her to become pregnant with his daughter. Darwish, who was already serving a six-year sentence for indecently assaulting ten other patients, was acquitted of rape during a court case in 2001.

Three young men ‘from respectable families’ were cleared of plotting to rape a Cambridge University graduate in 2001. Links to an earlier article in which one of the accused, Andrew Udenze, said the student ‘agreed to have sex’ minutes after getting into a car with him and four other strangers have also been taken down.

A British grandmother left her husband after thirty-eight years to marry a twenty-two-year-old Moroccan she met on the Internet, who was refused a visa by the Home Office three times.

A former advertising executive with Saatchi & Saatchi who left his family for a younger colleague was jailed for six months in 2000. After the younger woman left him, he was arrested and charged with harassment over bombarding her with phone calls, e-mails and letters.

A hotel manager hid £58,000 in stolen cash taken from her employers and recently married couples in bags and boxes under her bed, Newcastle Crown Court heard in 2002. She was jailed for nine months.

A pilot was killed during a fundraising flight for his village church in Dorset during 2009.

Google has also taken down a link to an online dating profile for user Thom109 on Telegraph Dating.

A homosexual vicar fled his parish after a campaign of blackmail and intimidation in 2000.

An “eccentric” sixth-former with a fascination for chemistry sparked a full-scale alert in 2005 after police found a cache of bomb-making chemicals in his bedroom.

Mother of two Teresa McKenzie was found unanimously not guilty of seven charges made against her by a sixteen-year-old male pupil, who alleged the pair had a ten-month relationship.

A “dapper” diamond thief killed his wife before hanging himself at their home in one of London’s most affluent postcodes in 2013.

A divorced businessman won a legal battle against his former wife in 2002, entitling him to an equal share of their £2.5 million fortune.

Back-office bank worker Adam Lancelot was prosecuted for fraudulently receiving benefits while being paid £300 a day in the City during 2012.
• British backpacker Alfred Alexandros Mill Saunders, twenty, was arrested on suspicion of murdering a woman in a frenzied, drug-fuelled knife attack in Central America in 2012.

• A former headmaster spat in a school governor’s face a decade after a row over scrapping “elitist A levels” in 2008.

• A 2002 article detailing how Britain’s Jewish community staged a 30,000 person-strong demonstration in Trafalgar Square to show support for Israel.

• “Absolute English gent” Hugh Taylor undertook a legal fight against Theresa Hamer over the return of some paving stones from a property Mr Taylor bought from Mrs Hamer for £3.5 million in 2002. Mrs Hamer removed the paving from a 282 square yard piazza on the property when she moved out, prompting Mr Taylor to appeal for the return of the “irreplaceable” stones.

• A 2004 article about the disappearance of 16 year-old Charlotte Pinkney from Ilfracombe, Devon. The teenager’s body was never found, and scaffolder Nick Rose was found guilty of her murder and jailed for life the following year.

• A company director killed himself while on Skype to his partner in 2011. Adrian Rowland was on a business assignment in India when he cut his own throat on camera while talking with his distraught partner in the UK.

• An article detailing how an RAF pilot was accused of sexually assaulting a female junior officer after creeping into her bedroom following a champagne party, a court martial heard in 2005. The link to a second article following his unanimous acquittal a week later has also been removed.

• A 2006 article detailing how an illegal immigrant was allowed by the Court of Appeal to stay in Britain because deporting her would breach her right to a family life with another woman.

• A 2003 article about people under thirty suffering strokes.

• Secretary Laura Cook kicked a fellow train passenger in the face with her stiletto following an argument. Ian Garven was attacked by Ms Cook and her boyfriend Nicholas Rogers after he asked Rogers to take his feet off the train seat. The pair were ordered to complete eighty hours’ unpaid work, pay £200 compensation and £250 prosecution costs in 2008.

• Celebrities were apparently reluctant to be seen with party organizer Nicholas Meikle, who was implicated in the alleged gang rape of a young woman by a group of men including Premiership footballers in 2003. Meikle was later cleared of any criminal wrongdoing.

• The boyfriend of Art Malik’s daughter was found dead in a swimming pool at the actor’s home in 2002.

• Mark Bruton-Young, thirty-six, an architect, allegedly murdered his daughter, Harriet, after he resented the intrusion of the “unplanned”
baby into his married life, Bristol Crown Court heard in 2011. He was later cleared.

• A Brazilian woman who claimed she lost her unborn twins in a knife attack by neo-Nazis was not pregnant and probably carved the initials of Switzerland’s main right-wing party into her own skin, Swiss investigators said in 2009.

• A Spanish court ordered an investigation into allegations that Saudi billionaire prince Alwaleed bin Talal raped a model on a yacht in Ibiza in 2008 be temporarily halted in 2012.

• A head teacher of a sixth-form college in Somerset wrote to students in 2010 asking them to support a member of staff who was preparing for a sex change.

• Selina Hakki was convicted of using rohypnol to drug wealthy-appearing men in order to rob them in 2004. She was sentenced to five years.

• An Oxford graduate who was among seven British tourists killed in a Nepal plane crash had been taking a final break before starting as an associate at a top City law firm in 2012.

• A sinister message was left on the mobile phone of a wealthy company director days after he was found shot dead in an orchard, an inquest heard in 2008.

• A businesswoman sacked after a night entertaining clients ended in spectacular embarrassment had her hopes of a compensation payout boosted by a tribunal ruling in 2012.

• A policeman’s daughter who willingly took part in sex and bondage with a former boyfriend made a false rape claim against him the next morning, a court heard in 2009. Links to a secondary article detailing the woman’s jailing for two years have also been taken down.

• The principal guest conductor for the English Chamber Orchestra Roy Goodman pled guilty to being in charge of a yacht while under the influence in 2004. Harbour officials saw him staggering on the deck of his new seven-metre yacht, RoyAnna, and urinating into the sea after it had run aground in one of Europe’s busiest shipping lanes.

• Nadia Almada’s entry in a Telegraph article of Big Brother’s most annoying housemates in 2011, in which she was described as “an annoying, unbearable nag.”

• A law student was convicted of killing and burying in concrete his controlling father who wanted him to study at the Sorbonne in Paris instead of living with his girlfriend in London in 2010.

• The younger sister of a schoolgirl who was raped and murdered by a serial sex offender leapt to her death from a multi-storey car park four days before her sixteenth birthday in 2009.

• A death announcement.

• A 2003 article detailing how the Roman Catholic Church reached a £15,000 out-of-court settlement with a former boy scout who claimed
he was abused by Fr. John Tolkien, the son of J.R.R. Tolkien, the \textit{Lord of The Rings} author.

- A 2012 article about twenty-seven-year-old Ben Ogden, who was killed in a plane crash in Nepal with six fellow British travellers.
- A computer hacker shut down America's biggest port when he took revenge on an internet chatroom user who had insulted his girlfriend, a court was told in 2003. A briefer version of the article has also been requested for removal.
- A woman planning a new life in Spain was knifed to death by an ex-lover who she had told police was stalking her, a court heard in 2010.
- A 2003 column by Jenny McCartney speculating whether men, including actor Hugh Grant, said they wanted children purely to bed women.
- A senior manager at a leading London law firm who wanted to work part-time, including half a day a week from home, after having a baby won her claim for unfair dismissal in 2005.
- City trader Asif Turabali Mohamedali, who confided in his boss that he felt suicidal, was told: "Tough luck, dude—pull yourself together," an employment tribunal heard in 2012.
- A senior Goldman Sachs banker went on holiday with his wife and five children to Bermuda and hoped to arrange for his mistress and her children to stay at a nearby hotel on the island at the same time, a court was told in 2004.
- An article detailing how a British man was jailed for twenty-five years in Costa Rica for stabbing to death a Czech student at a remote jungle eco-farm in 2013. Google also removed links to three images related to the story, found here, here and here. Numerous links to other articles, including the shock of the man's family, and how he was initially held in custody, have also been removed.
- A policeman who was a former British international runner announced his intention to sue Lancashire police for racial discrimination after the force spent three years and an estimated £450,000 investigating allegations that he overcharged his expenses by £90 in 2006.
- A detective who sparked an armed siege inside a police station after allegedly threatening to kill a colleague appeared in court in 2010.
- A 2004 article by Jenny McCartney about Frank Oz's remake of \textit{The Stepford Wives}.
- A Muslim teenager made up a rape story to cover her shame after losing her virginity to a married doctor, a court was told in 2003.
- A solicitor breached insider-trading laws when he tipped off his father-in-law that his company was about to be taken over by Motorola so the pair could make a £50,000 profit from buying and selling shares, a court was told in 2009. The link to a related article of nine ex-
amples of the FSA’s convictions for insider trading, including this case, has also been removed.

• A 2011 liveblog of a Cricket World Cup match between India and England, manned by Rod Gilmour and Jonathan Liew.

• An article recounting the story of a Kosovo-born Muslim and her fight against deportation from Holland, written in 2006.

• An 2014 interview with a British mother of twins, whose estranged husband was awarded full custody of the children by an Austrian family court, despite social workers’ recommendations she be granted sole custody due to his violent and unpredictable behaviour.

• A maid who claimed she had been beaten and kept as a slave by her employers faced prosecution after an employment tribunal ruled she invented the abuse in 2010.

• A glamour model and reality TV star who told police her BlackBerry had been stolen after she left it at the gym was spared jail in 2010.

• An 2005 article and related image regarding how a murdered heiress had called off her wedding a fortnight previously.

• Two primary school teachers were cautioned for branding an eight-year-old pupil a “chav” on Facebook in 2008.

• A leading researcher into heart disease escaped jail in 2004 after a court heard that he slapped his fiancée and broke a hotel deputy manager’s arm in a drunken rage on the eve of his wedding.

• A banker was one of the chief organisers of the drinking-ban protest on the London Underground which descended into violence in 2008.

• A director was jailed for eight years in 2006 for stealing more than £34m from Izodia, a one time dotcom-boom company that became a cash shell.

• A feature exploring the anatomy of a £34m theft from 2007, surrounding the arrest of Dr. Gerald Smith.

• A leading psychologist tried to kiss a male colleague at a dinner and then tried to stroke another man’s thigh in front of his bemused wife, a hearing was told in 2010.

• An article from 2004 about overly pushy parents accompanying their children to university.

• A yachtsman who was overpowered and tied up by two friends during a storm in the Bay of Biscay had “lost it” after several days without eating or sleeping properly, Spanish police said in 2004. The link to a related brief news story explaining how no further action was to be taken against the trio has also been removed.

• An article relating to the fallout between former Environment Secretary Caroline Spelman and her teenage son’s desire to become a body-builder from 2012.

• A policeman whose assault on a man was filmed by CCTV cameras was jailed for twenty-one months in May 2003.
Two articles from August 2014 and November 2014 about how a lawyer-turned-sailor claimed sexual discrimination and harassment against organisers of gruelling race but had her case thrown out.

A former care assistant in an old people’s home was jailed in 2004 for helping her lover to rob elderly women.

A former world-boxing champion was jailed for two and a half years in 2003 after he was caught with £21,000 worth of cannabis in his car.

A 2006 story about the arrest of two chief executives of an Austrian gambling firm.

A mother sued her former solicitor for £15m in 2013, claiming his poor advice cost her millions of pounds in a divorce settlement.