Forget About the Right to be Forgotten: How About a Right to be Different?

AMANDA CHENG *

Every day, people conduct Google searches. More often than people would admit, these searches are for specific individuals. As users, we wish to uncover as much information as possible about the people we search. But as data subjects, we wish to retain our privacy and keep our past in the past. Concerns about data protection, privacy and reputation curation will only accumulate as we spend more time online. To address these concerns properly, we need to rise above scaremongering about the right to be forgotten. We must think critically about how we want to use the web, and find practical ways to balance the competing interests at play. To this end, this article critically analyses the Court of Justice of the European Union’s 2014 judgment Google Spain v Agencia Española de Protección de Datos, as well as the General Data Protection Regulation. It suggests that the right to be forgotten should be replaced with a “right to be different” — a solution that heavily emphasises worldwide applicability, permanence and longevity.

I PREFACE

A happy couple give birth to X. In celebration, the new parents post an announcement on Facebook. Days later, the rookie father makes a mess changing diapers. He posts a humorous but graphic story about this on his blog. At the age of 16, X attends a party, unbeknownst to his parents. He sneaks out with their expensive sports car and drunkenly crashes into a neighbour’s fence. The neighbour uploads photos of the incident to Facebook, which are later used by

* BMus, LLB(Hons). Solicitor, Chapman Tripp. I would like to thank Judge David Harvey for his extensive insight; my friends for their unwavering support; and, most importantly, my family for encouraging every interest and endeavour I pursue.
newspapers online. X is now 23 years old and wants to apply for a graduate job.

Y’s father is abusive, and her mother is a drug addict. Her parents’ violent history has regularly been documented in the local newspaper; its archives have recently been digitised. Despite this childhood of hardship, Y is now embarking on an academic career as a university lecturer.

A celebrity couple adopt baby Z. Z’s father is a real estate tycoon and his mother is a movie star. Due to his parents’ public lives, Z’s health problems are public knowledge and frequently feature on tabloid websites. At age 27, Z is suspected of operating a Ponzi scheme, but investigations were inconclusive. Now aged 40, Z is looking to start a new investment company.

Should X, Y and Z be able to erase the undesirable elements of their past by preventing them from appearing in online search results?

II INTRODUCTION

Humans are not static beings. Our life changes can vary from the mundane and inconsequential, like a child choosing a new favourite colour, to the outrageous and deeply shameful, like a former Subway spokesman becoming embroiled in a child pornography ring.¹

Increasingly, we share and re-share every element of our lives online. From graduation photos to car accidents, attaining good grades to bar fights, people thoughtfully — or carelessly — document their lives and the lives of those around them on the World Wide Web (“the web”). Although people change, representations of their lives and identities may remain unchanged and permanently online. As such, a youthful mistake may cause distress or recurring punishment indefinitely into the future.²

This article focuses on the “right to be forgotten” in the form of removing Uniform Resource Locators (URLs)³ from the search results for named individuals. It aims to examine the power struggle between the online sphere as a vehicle for free-flowing information, and its users’ desire to lead lives unfettered by the ghosts of their past. The core of this topic is the paradox of Theseus:⁴ is someone still the

² See Daniel J Solove The Future of Reputation: Gossip, Rumor and Privacy on the Internet (Yale University Press, New Haven (Conn), 2007) for examples of “punishment” resulting from online representations.
³ A Uniform Resource Locator (URL) is the address of information or a collection of information located on the web. A URL’s main function is to point to a specific web page.
⁴ See Michael Clark “Paradoxes 1: The Ship of Theseus” (2002) 1(1) Think 75.
same person if he or she has fundamentally changed? The current legal position is inadequate to deal with this “very real problem”. The various solutions proposed by academics rely on pre-existing law, heavily restricting the potential to achieve a permanent and trans-jurisdictional solution. This article will draw on two pre-existing concepts — “contextualisation” and the “right to be different from oneself” — but will reframe them in a more sustainable way. Ultimately it will propose a right to be different, rather than forgotten.

Briefly, the concept of a right to be different focuses on the human reality that people change, and as such, information online ought to change with them. But it also respects the dangers of censorship and erasing “the past”. The emphasis is on informational integrity — while a past event may not be justifiably “forgotten” from the web, more up-to-date information can help to counteract the dangers of a contritely frozen online representation of an individual. The right to be different does not weigh the value of an individual’s past self against his or her present self; the aim is instead to preserve the narrative of events and people’s lives.

III BACKGROUND

The starting point for this discussion is Google Spain v Agencia Española de Protección de Datos, in which the Court of Justice of the European Union (CJEU) ordered that URLs be removed from search results for the plaintiff’s name. The full facts of the case are set out below. This section of the article provides an introduction to the key concepts underpinning the decision.

8 An understandably popular conceptualisation of the right to be forgotten is “forgive and forget”, in which forgetting is essential to forgiveness. This article does not incorporate forgiveness into the solution because a “fault” or prejudicial element is unnecessary to trigger the right to be forgotten. See generally Sanna Kulevska “Humanizing the Digital Age: A Right to Be Forgotten Online?” (LLM Thesis, Lund University, 2014) at 13; Rustad and Kulevska, above n 6, at 352 and 416; Emily Adams Shoor “Narrowing the Right to Be Forgotten: Why the European Union Needs to Amend the Proposed Data Protection Regulation” (2014) 39 Brook J Intl L 487 at 514 and 517; Jeffrey Rosen “Free Speech, Privacy, and the Web that Never Forgets” (2011) 9 J on Telecomm & High Tech L 345 at 354; and Michael Douglas “Questioning the Right to Be Forgotten” (2015) 40 AitLJ 109 at 112. See also s 19 of the Harmful Digital Communications Act 2015 [HDCA], which enables a court to order removal of a harmful digital communication or grant a right of reply. However, the HDCA only focuses on harmful content posted by third parties. Because harm is not a requirement for triggering the right to be forgotten, this article does not discuss the HDCA.
9 Case C-131/12 Google Spain SL v Agencia Española de Protección de Datos [2014] 3 CMLR 1247 (CJEU).
Definitions

In this article, “Google” refers to both the global technology company and the concept of “search engines”. Google is the most prominent and ubiquitous search engine. People do not “Yahoo” things; instead, they “Google” to find information. Due to the ever-increasing size and complexity of the web’s contents, search engines are crucial in facilitating its access and navigation. By allowing relevant URLs to be located upon a keyword search, search engines bring order to the web’s inherent disorganisation. The search engine results page is produced using “sophisticated computer algorithms.” In theory, this process is automated, and Google prides itself on this assertion.

In this article, the “right to be forgotten” refers to “delisting”, which is the removal of one or more URLs from a search engine results page. The right to be forgotten applies primarily to searches for an individual’s name but may also affect searches that contain names in combination with other words.

Data Protection and Privacy

The relationship between data protection and privacy is complex: while overlapping in theory, they remain legally distinct. Further, both data protection and privacy are concepts that vary markedly between jurisdictions.

1 Legislative Framework

The jurisprudence of data protection and privacy in Europe is confusing as there are two complementary legislative frameworks. These frameworks are not mutually compatible in their treatment of the two concepts.

First, the European Convention on Human Rights (the Convention) binds all European Union (EU) Member States, as well as other non-Member States which are in the Council of Europe

---

11 The verb “Google” is in the Oxford English Dictionary (online ed, Oxford University Press, 2006).
12 Grimmelmann, above n 10, at 940.
13 At 950.
14 At 943–950. However, this is not always the case. Google manually delists many URLs to comply with US copyright legislation. See Part IV, “Reactions to the Case”.
15 See Part V, “Censorship and Freedom of Expression”.
16 Juliane Kokott and Christoph Sobotta “The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR” (2013) 3 IDPL 222; and Maria Tzanou “Data protection as a fundamental right next to privacy? ‘Reconstructing’ a not so new right” (2013) 3 IDPL 88.
The Convention’s judicial body — which adjudicates on human rights breaches — is the European Court of Human Rights (ECtHR).

Secondly, the CJEU oversees the protection of fundamental human rights in Member States. These rights are enshrined in the Charter of Fundamental Rights of the European Union (the Charter). The CJEU’s interpretation of the Charter follows the ECtHR’s views on the Convention and the ECtHR also takes the CJEU’s interpretations into account.

The Convention does not explicitly address data protection, but protects a general right to privacy, namely, a “right to respect for … private and family life”. It states that no public authority may interfere with this right “except … in accordance with the law … or for the protection of the rights and freedoms of others”.

In contrast, the Charter explicitly provides for the “[p]rotection of personal data”. Article 8(1) states that “[e]veryone has the right to the protection of personal data concerning him or her”. This is a form of informational privacy, and appears to expand on art 7, which states that “[e]veryone has the right to respect for his or her private and family life, home and communications”. Article 8(2) further states:

Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Strangely, the CoE’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data also specifically includes data protection of personal data, despite not being in the ECtHR’s jurisdiction.

---

19 Kokott and Sobotta, above n 16, at 222–223.
20 Convention, above n 17, art 8(1).
21 Article 8(2).
22 Charter, above n 18, art 8.
23 Article 8(1).
24 Article 7.
2 The 1995 Data Protection Directive

Until 2016, the EU’s primary legal instrument for data protection was the 1995 Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (the Directive). Interpretation of this Directive formed the legal basis of Google Spain. The relevant principles of data protection are:

(1) Personal data shall be processed fairly and lawfully.
(2) Personal data shall be obtained only for ... lawful purposes, and shall not be further processed in any manner incompatible with ... those purposes.
(3) Personal data shall be adequate, relevant and not excessive in relation to the ... purposes for which they are processed.
(4) Personal data shall be accurate and, where necessary, kept up to date.
(5) Personal data processed for any purpose ... shall not be kept for longer than is necessary ....
(6) Personal data shall be processed in accordance with the rights of data subjects under the [Directive].

“Personal data” is defined as “information relating to an identified or identifiable natural person”. The “data subject” is the person to whom the personal data relates. A data “controller” “determines the purposes and means of processing” other data subjects’ personal data, and a data “processor” processes this data on the data controller’s behalf. A data controller and data processor are separate legal entities.

Due to the Directive’s age, there is a large disparity between the situations envisioned at the time of adoption and today’s technological realities. The EU recently adopted the General Data Protection Regulation (GDPR), aiming to bridge the gap between the

26 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 [Directive].
28 Directive, above n 26, art 2(a).
29 Article 2(a).
30 Article 2(d).
31 Article 2(e). Article 4(2) defines “processing” as “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction”. The definition is extremely broad, designed to cover any and every action — even inaction — applied to personal data.
32 European Union Agency for Fundamental Rights, above n 18, at [2.3].
principles established in 1995 and today’s practices. The GDPR is discussed further in Part VI.

3 Privacy

A founding principle behind privacy is the protection of the “right to be let alone”. Privacy law aims to prevent harm or offensiveness, which must be weighed against competing claims of freedom of expression and public interest. Despite this relatively simple distillation, privacy is difficult to define in both philosophical and legal terms. The lack of a satisfactory definition along with the ever-changing technological landscape means that privacy is increasingly difficult to regulate.

At first glance, the established right to privacy is of limited relevance to the right to be forgotten. Privacy involves “non-disclosure of personal information to third parties, including into the public domain”. The right to be forgotten, in contrast, attempts to limit access to facts that are already in the public domain.

Newer ECtHR jurisprudence acknowledging a “legitimate expectation” of privacy in public places may give privacy renewed relevance in analysing the right to be forgotten. At its core, this jurisprudence suggests that “a rigid distinction between that which takes place in private and […] in a public place” is no longer determinative of whether there is a right to privacy. Nevertheless, the issues in this article are not explored through privacy law as Google Spain rests on a data protection instrument. This article ultimately proposes that a solution for these issues — whether of privacy, data protection or social permanence — should be not be constrained by the artificial boundaries between these concepts.

33 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1 [GDPR].
35 See generally Hosking v Runtig [2005] 1 NZLR 1 (CA).
38 At 12.
4 Differences Between Data Protection and Privacy

Although they are often confused or used interchangeably, data protection and privacy are different concepts.

(a) Scope

Data protection is limited to individuals. It covers everything from “sensitive” data to mundane information about an individual. “Sensitive” data is data concerning an individual’s racial or ethnic origin, political views, religious beliefs, sexual orientation or conduct, trade union membership or health. Mundane information could be about anything, for example, what food the data subject ordered. However, “sensitive” data is subject to higher protection, the default position being that sensitive data is forbidden from being processed.

Privacy law, on the other hand, covers only information that is “sensitive”: the disclosure of information that is merely “private” but not “sensitive” does not give rise to legal liability. It is strictly about the acquisition, storage, or disclosure of information, while data protection focuses more on the use of information and whether that use will affect an individual.

(b) Source

The sources of the two rights are very different. Privacy as a right has no clear source, and the concept differs wildly between jurisdictions. Conversely, the European data protection rules arose directly from post-Second World War concerns about the Nazis’ use of data and the threat of “automated data processing”. For example, in the 1930s, the Netherlands had a population registry designed for “government administration and improving welfare planning”. It contained the “name, birth date, address, religion, and other personal information for...
each citizen”. However, when the Nazis invaded, this registry was repurposed, allowing the Dutch Jewish population to be persecuted more efficiently than those in any other European nation. European data protection rules also responded to a fear that decisions made based on automated data processing would be prejudicial, and that out-of-date or incomplete information could spawn further prejudice.

(c) Effect

Whereas privacy is concerned mainly with information disclosure, data protection does not seek to merely keep information private. Data protection seeks to control the content of information, as well as what is being done to or with the information — in other words, informational autonomy. The principles in the Directive reflect this. The German Constitutional Court held that the principle of “informational self-determination” protects the individual’s power to decide when his or her data may be used or disclosed. Article 2 reflects this by requiring that consent for data processing be specific, informed, freely given and unambiguous.

Data protection therefore offers objective protection, rather than the subjective protection of privacy. While an individual must prove that something is “private” to be protected by privacy laws, a piece of information does not need to be deemed “private” for data protection rules to apply — simply being personal data is sufficient. There is therefore little flexibility in whether data protection rules apply. In contrast, Member States have a greater “margin of appreciation” in conceptualising the limits of art 8’s right to privacy. Notably, they have the flexibility to balance privacy rights against art 10’s right to freedom of expression.

Ultimately, neither data protection nor privacy rights are absolute, but the ways in which they are circumvented are different. These nuanced characteristics of data protection law formed the basis of Google Spain.

49 At 141.
50 At 141.
51 As set out above in Part III, “Data Protection and Privacy”.
52 Volkszählungsurteil (1983) 65 BVerfGE 1 at 68–69 as cited in Tzanou, above n 16, at 89.
53 Directive, above n 26, art 2(h).
54 The concept of a “margin of appreciation” is discussed in Mahon v Keena [2009] IESC 64 at [47]–[62]. See also Lisbon Network “The Margin of Appreciation” Council of Europe <www.coe.int>.
IV HARD CASES MAKE BAD LAW — THE HARD CASE

On 13 May 2014, the CJEU handed down *Google Spain*, a judgment that many people around the world — especially journalists — found controversial. Ignoring the fact that the judgment is only binding in the EU, at the time of the judgment, media outlets and their comment sections became awash with outrage. For the first time, a court found that an individual had, in certain circumstances, a right to be “forgotten” from Google search results.

A brief consideration of the comment sections of news websites is sure to leave one feeling dismayed. While much of the outrage directed at the *Google Spain* judgment was based on ignorance rather than facts, one commenter posed pertinent questions piercing the heart of the judgment’s problems:55

Is an MP appearing on BBC Breakfast a public figure?
Is the presenter of BBC Breakfast a public figure?
How about the presenter of the BBC regional news?
Someone who once appeared on the regional news?
A journalist working for a national newspaper?
A journalist working for a local newspaper?
A student writing articles for their student newspaper?
Someone who once wrote an article in a school newsletter?

The *Google Spain* judgment is ambiguous and difficult to apply, so what guidelines did the CJEU provide?

Facts

The case originated in Spain in 2010 when Mr Costeja González lodged a complaint against a newspaper, *La Vanguardia*, with the Agencia Española de Protección de Datos (AEPD), the Spanish data protection agency. Mr Costeja González complained that when his name was searched on Google, the results showed links to two articles in *La Vanguardia*’s digitised archives. These articles dated back to 1998, and were related to real estate auctions for the purposes of recovering social security debts. As the announcements for the auctions were published not only legally, but also under statutory order by Spain’s Ministry of Labour and Social Affairs, the AEPD could not order the removal of the original web pages. The Spanish court referred the case to the CJEU on three issues:

55 tjunction, as commented on 13 May 2014 at 11:31 on Alan Travis and Charles Arthur “EU court backs ‘right to be forgotten’: Google must amend results on request” *The Guardian* (online ed, London, 13 May 2014).
(1) whether the Directive applied to search engines such as Google;
(2) whether the Directive applied to Google Spain, whose data processing server was in the United States; and
(3) whether an individual has the right to request removal of personal data from a search engine.

In summary, the CJEU found that the Directive applied and that EU data protection law also applied to search engines. The CJEU also found Google to be a data controller, and interpreted art 12(b) of the Directive to grant individuals a right to be forgotten from search engines. Despite the judgment being a victory for Mr Costeja González, the original data still remains on the La Vanguardia website. As such, the judgment did not raise as many concerns about freedom of expression as a traditional action for removal would have done. Yet as will be discussed later, the removal of URLs from search engine results does amount in practice to censorship. This irreconcilable gap between the practical and technical consequences of Google Spain is important. And dangerous.

Issues 1 and 2 are outside this article’s scope and will not be examined. Whether the judgment is legally sound is also outside the scope of discussion. The focus of this article will be on the issues that arise as a result of the judgment.

The Google Spain Right to be Forgotten

The CJEU found that, pursuant to art 12(b) of the Directive, the inclusion of the two links to La Vanguardia under searches for Mr Costeja González’s name would be incompatible with the Directive’s data protection principles. Accordingly, Mr Costeja González had the right to have the relevant URLs delisted from the search results. To qualify for this right to be forgotten, a data subject must show that:

(1) the URLs that the data subject wishes to delist from search engines are “inadequate, irrelevant or no longer relevant, or excessive”; and
(2) the data subject does not have a public life which would generate enough public interest to justify interfering with his or her privacy.

56 Google Spain, above n 9, at [41].
57 At [70].
58 At [94]. The Directive’s key data protection principles are set out in art 6.
59 At [94].
The problem with the above criteria is that the CJEU used concepts of privacy to grant Mr Costeja González a right to be forgotten from Google search results, but purported to acquire legal power from a data protection directive. This is where the judgment’s legal conceptualisation of the right to be forgotten becomes confusing. It clearly demonstrates how data protection and privacy are difficult to distinguish. Notably, although Google Spain was a case regarding the interpretation of the Directive, one of the judgment’s key paragraphs points to arts 7 and 8 of the Charter, the provisions concerning privacy.61

The CJEU added that to meet the above criteria, the “information in question” need not cause “prejudice to the data subject”.62 This means the links that EU residents are entitled to request be delisted do not necessarily need to be anything “bad”. The judgment also stated that the data subject’s right to be forgotten overrides the “economic interest” of the search engine’s operator.63

Reactions to the Case

Julia Powles considers Google Spain a triumph for individual rights. She argues that the case “does not just blithely fold to practical concerns … it attempts to give real recognition to the interests of individuals”.64

This is undoubtedly correct. Google Spain recognises that digital rights and privacy in the ever-expanding online sphere are increasingly important. Intermediaries such as Google have been crucial in protecting corporate economic rights — such as copyright — and it is encouraging to see that human rights online are now gaining traction.65 It would be wrong for individual rights to be ignored online while copyright is vehemently protected. Each day, Google delists countless URLs, across all its international domains, to comply with US copyright legislation.66 Unlike the Google Spain decision, delisting to protect copyright has not been met with outrage. This seems odd, given the prevalence of online piracy.67 Indeed, one might expect many web users to be concerned more about loss of their

60 At [97].
61 At [97].
62 At [96].
63 At [97].
64 Julia Powles “What we can salvage from ‘right to be forgotten’ Ruling” Wired (UK) (online ed, London, 15 May 2014).
65 Powles, above n 64.
67 See Anna Kukla-Gryz and others “We all do it, but are we willing to admit? Incentivizing digital pirates’ confessions” (2015) 22 Applied Economics Letters 184 and the articles cited therein.
free entertainment sources than about loss of access to information relating to a stranger’s decades-old debts, which are now of no consequence to others.

Ill-informed criticism over *Google Spain* claims the judgment will allow politicians or serious criminals to hide their past. This criticism is unfounded because such individuals would not meet the second criterion, as there would be sufficient public interest to justify interfering with their privacy.

Another frequently criticised aspect of the case is that Google, rather than local data protection authorities, is responsible for processing and determining delisting requests. There certainly are issues with Google having sole responsibility for determining delisting requests with limited oversight, as discussed below in Part V, “Transparency”. However, it should be acknowledged that Google *does* have better resources than EU Member States’ local data protection authorities to process such requests.68 Furthermore, Google can implement any decision it makes immediately, without having to wait for an intervening judicial body.

Although the issue of whether Google is a data controller is outside the scope of this article, it is important to note the CJEU had its hands tied in this finding. Under EU law, any entity that processes data is either a data processor or a data controller.69 Even if the CJEU did not believe that “data controller” was the perfect legal category for a search engine, the Court can only base its rulings on pre-existing European law.70 The CJEU was unable to invent a separate category — it was only able to find that Google was a data controller, data processor or neither. Despite the finding’s impracticalility, holding that Google was not a data controller would have been contrived. This would have meant a data subject has no rights against Google and therefore no remedy against outdated information on the web.

### V HARD CASES MAKE BAD LAW — THE BAD LAW

The often-overlooked fact in *Google Spain* is that the *La Vanguardia* publications associated with Mr Costeja González were *statutorily*

---

68 For a discussion on the benefits of Google processing delisting requests, see Edward Lee “Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten” (2016) 49 UC Davis Law Review 1017 at 1078–1083; and Michel J Reymond “Finding common standards for the Right to be Forgotten: Challenges and Perspective” (Luncheon Series presented to Berkman Klein Centre for Internet & Society at Harvard University, Cambridge, 4 May 2016) <cyber.law.harvard.edu/luncheons>.


70 “Internet Policy Forum Debate”, above n 69, at 50:26 onwards.
ordered. Most newspaper articles would not be statutorily ordered, and this is perhaps why a case like this did not come before the CJEU until 2014. Despite this, the CJEU’s findings have broad application, leaving Google, the EU and the rest of the world with an outcome both difficult to accept philosophically and difficult to implement.

Amidst Europe’s arguments surrounding data subjects’ rights to privacy and the right to control personal data, one must remember that the right to be forgotten applies to truthful, legally-obtained information that is already in the public sphere. Powles wrote, “[a]t best, [Google Spain] is reckoned to be hopelessly unworkable. At worst, critics pan it as censorship”. So, how bad is Google Spain’s right to be forgotten?

Territoriality

The web is global. It does not have boundaries that are regulated easily — or at all — by legal jurisdictions defined by borders and territories. As Rustad and Kulevska point out:71

Data packets containing personally identifiable information do not report to customs when they cross national borders on the virtual highway; routers do not pause to consider whether privacy norms are being breached.

Google Spain is binding only in the EU. However, the French data protection agency wanted Google to apply delisting across all of its domain extensions internationally.72 Initially, Google staunchly resisted this and complied with Google Spain only on its EU domains, leaving results on its non-EU domains such as Google.com.73 As a result, users could circumvent Google Spain’s effects by using a non-EU Google domain to conduct a search. While partially ameliorating criticisms that the decision led to unjustified censorship, this avenue for circumvention was seen also as a hindrance in achieving the aims of the judgment. Sadly, Google abandoned its resistance in March 2016,74 applying delistings across all of its domains. This was despite

71 Rustad and Kulevska, above n 6, at 386.
73 Nadège Martin and Amelie Mervant “Google challenges applicability of CNIL’s ‘right to be forgotten’ order to domain extensions outside the EU” (4 August 2015) Data Protection Report <www.dataprotectionreport.com>. See also Peter Fleischer “Implementing a European, not global, right to be forgotten” (30 July 2015) Google Europe Blog <www.googlepolicyeurope.blogspot.co.nz>, in which Google maintained that EU-only implementation was sufficient as an “overwhelming majority of French internet users” — “around 97%” — access Google using Google.fr, Google’s French domain extension, rather than other international domain extensions like Google.com.
74 Peter Fleischer “Adapting our approach to the European right to be forgotten” (4 March 2016) Google Europe Blog <www.googlepolicyeurope.blogspot.co.nz>.
the previous statement of its Global Privacy Counsel “that no one country should have the authority to control what content someone in a second country can access”. 75

Some commentators, however, are supportive of Google’s change of heart. Paul Nemitz believes that it is a “huge mistake … to assume that Google defines geography”, or, for that matter, that domain extensions define geography. 76 It is true that domain extensions can be seen as artificial constructs that distort the reality that the web does not have borders. A person in New Zealand can register a .co.uk domain name just as a European resident can register a .com domain name. The Article 29 Working Party recognised this loophole and consequently stated that confining delisting to EU domains “cannot be considered a sufficient means to satisfactorily guarantee the rights of data subjects according to the judgment”. 77

Censorship and Freedom of Expression

A popular analogy for the right to be forgotten likens Google search results to a library catalogue. 78 Proponents of the right to be forgotten claim that delisting does not amount to censorship as the original web page remains online, similar to leaving a book in the library but removing it from the catalogue.

Frankly, this is a naïve metaphor. In a physical library, users may walk to a shelf containing a book they want. They may then peruse the vicinity, knowing that books are grouped by subject matter, and they will likely find other books of similar interest. But this is not how the web works. The web is far larger and messier than a physical library. The closest comparison would be to take all the books in the world and mix them up: “declassify” them by removing the Dewey catalogue system. A more extreme equivalent would be to tear out all pages from books and jumble them at random. This would be a closer physical approximation of web browsing without search engines. How does one find a book, or a specific page of a book, if one does not know that the book exists?

Therefore, despite the original publication remaining on the web, delisting may still amount to censorship. First, URLs are

75 Fleischer, “Implementing a European, not global, right to be forgotten”, above n 73.
76 Paul Nemitz, speaking to the Advisory Council to Google on the Right to be Forgotten (Brussels, 4 November 2014). Transcripts of the Advisory Council’s meetings are available at <www.google.com/advisorycouncil>.
78 See, for example, David Drummond “We need to talk about the right to be forgotten” The Guardian (online ed, London, 10 July 2014).
removed not only from the search results of a “first name–last name” query, but also from results of “queries that include the person’s name”. 79 For example, Danny Sullivan demonstrated that if “Emily White” were granted delisting by Google, then the delisted URLs would also be delisted from results of queries such as “Emily White bankrupt”. 80 This goes beyond simply making it difficult to locate information — it blatantly hides information. While a passer-by in Emily’s life should not necessarily be privy to Emily’s past bankruptcy, an individual specifically looking for information regarding the bankruptcy ought to be in a different user category. Practically, it would be very difficult to administer a motives-based gateway to search results — should only a search for “Emily White bankrupt” reveal such information or would “Emily White financial issues” suffice? It would also pose difficult legal and moral questions. Yet delisting based on any search including the data subject’s name draws a darker, wider curtain over an individual’s life than is necessary. Such delisting may remove “indispensable data”, creating incomplete narratives which may “delay investigations” by journalists. 81

Outside the EU, freedom of expression is protected statutorily and culturally to a higher degree than privacy. Perhaps this is because freedom of expression is an easier right to conceptualise than privacy, and more central to the ideals of democracy. In New Zealand, freedom of expression is enshrined in s 14 of the New Zealand Bill of Rights Act 1990. Similarly, the United States protects freedom of expression in the First Amendment to the Constitution.

All major media outlets now produce news for online consumption. The abundance of content being published online means simply publishing content is no longer an effective means of dissemination. If a page is not searchable on Google, then for all practical intents and purposes, it may as well not exist. The late Aaron Swartz considered Google to be a “gatekeeper” that “tell[s] you where on the internet […] to go”. 82 He explained that, since the world no longer has broadcasting limitations such as a maximum number of radio frequencies, “everyone can have a channel … everyone has a

---

79 Chris Moran, speaking to the Advisory Council to Google on the Right to be Forgotten (London, 16 October 2014); and Google “Privacy & Terms — FAQ” <www.google.ie/policies/faq> [Google FAQ].
81 Rustad and Kulevska, above n 6, at 373–374. Initially, the main counterargument to the censorship issue was that Google only applied the Google Spain requirements to its EU domains. A user could therefore still find the “delisted” URLs from non-EU domains such as Google.com. However, as discussed in Part V, “Territoriality”, this practice ended, and the delisting is now applied across all domains.
way of expressing themselves [online]”. As a result, it becomes “a question of who gets control over the ways you find people”, and “power [centralises] in sites like Google”. The result is that “everyone has a licence to speak — it’s a question of who gets heard”. In Europe and much of the world, Google is “the” search engine, which means that if a page cannot be found on Google, it is unlikely to be found at all. Drawing from this, we might ask: is the “open justice” principle met if court proceedings are published but unable to be located — and thus practically non-existent? One could argue that if someone wanted to look for court proceedings, they may access law reports. However, if results are delisted, it may be difficult for the modern public to discover the court proceedings’ existence in the first place.

Overall, Google search results summarise what is “out there”. The right to be forgotten comes at the expense of the right to freedom of expression, despite the original web page being left intact. The exact technical position is unimportant if the practical reality is censorship. The Irish Supreme Court has held that “justice … shall be administered in public”, and that media coverage is necessary to fulfil this requirement of having a “public” court.83 As such, if the practical reality is obscurity, this amounts to censorship as the public cannot easily access such information. Similarly, The Guardian considers Google to be “the front page of [its] whole archive”.84 Chris Moran, The Guardian’s Audience Editor, stated that in the week prior to Google’s Advisory Council forum in London, The Guardian “received over 20 million page views from Google, over half of that to content that [was] more than a week old”.85 This demonstrates just how crucial Google is for page views and attention.

Transparency

There are three main transparency issues arising out of Google Spain. First, the CJEU allocated Google the responsibility of internally evaluating delisting requests. Secondly, there is no requirement for Google to inform the publisher or webmaster of the delisting. Thirdly, the public are left in the dark about Google’s in-house evaluation process. This third issue will be dealt with under Part V, “The Balancing Test”.

A tangential issue is that Google displays a notice stating that “results may have been modified in accordance with data protection

84 Moran, above n 79.
85 Moran, above n 79.
Forget About the Right to be Forgotten: How About a Right to be Different?

law in Europe” when a user searches for “most names”. 86 This means that the message also appears on names where no delisting has occurred, leading to a shroud of secrecy. However, names of celebrities or famous politicians do not trigger the same disclaimer as they clearly fall outside the ambit of Google Spain due to their “public life”. 87

1 Internal Review of Requests

There is no judicial body in the world with “the resources to deal with [the] volume of work” generated as a result of Google Spain. 88 However, it is a “real concern” that the CJEU shifted oversight and enforcement of human rights to a corporate entity. 89 This gives Google considerable power, and burdens it not only financially, but also with the obligation to “get it right”. It is against the rule of law that Google is not only a party, but also “judge, jury and executioner”. 90

A group of 80 “internet scholars” wrote an open letter to Google calling for more information about the implementation process and disclosure of statistics regarding both accepted and denied requests. 91 They believed that implementation of Google Spain should be more transparent because: 92

(1) the public should be able to find out how digital platforms exercise their tremendous power over readily accessible information; and (2) implementation of the ruling will affect the future of the [right to be forgotten] in Europe and elsewhere, and will more generally inform global efforts to accommodate privacy rights with other interests in data flows.

Although Google’s decisions “seem reasonable”, it is currently impossible to evaluate how the decisions are being made and implemented. 93 While Google “looks like a public utility, it is not a public utility” — it is a company “driven by profit”. 94 Compliance with Google Spain entails a hefty cost which Google “will try to minimise”. The fear is that it is easier (and less costly) for Google to

---

86 Google FAQ, above n 79.
87 Jennifer Baker “Google’s ‘right to be forgotten’: One rule for celebs, another for plebs” (6 August 2014) The Register <www.theregister.co.uk>; and Google Spain, above n 9, at [97].
88 Douglas, above n 8, at 110. 89 At 110.
92 “Internet Scholars’ Open Letter”, above n 91.
93 “Internet Scholars’ Open Letter”, above n 91.
94 Douglas, above n 8, at 110.
accept rather than deny requests.\textsuperscript{95} This is because denying a request opens Google up to review by the local data protection agency and could lead to litigation.

Whatever merit Google Spain has as a “triumph for individual rights” is undermined when the responsibility for protecting these rights are handed to a corporate entity. The calls for transparency in the internet scholars’ open letter have been echoed by Google’s own Advisory Council and the EU’s Article 29 Working Party.\textsuperscript{96}

2 Notice to Publishers or Webmasters

Google Spain does not require Google to give publishers or webmasters notice of a delisting request or decision. This hinders both transparency and freedom of expression because Google is able to remove information from its results page without obtaining both sides of the story. In an attempt to mitigate this problem, Google has established its own notification policy. But Google’s compliance with this policy is neither mandatory nor monitored. There is still no independent assessment of delisting requests, making it difficult to assess the integrity of Google’s processes. Moreover, the CJEU did not prescribe a formal appeal process for webmasters or publishers wanting to resist delisting. Therefore, while publishers can “request that [Google] re-review a decision”,\textsuperscript{97} there is no formal appeal process to pursue. If Google disagrees, that is the end of the line for publishers.

The Balancing Test

In considering each delisting request, Google must conduct a balancing test between “personal privacy and access to information”.\textsuperscript{98} Apart from the two criteria discussed above,\textsuperscript{99} the CJEU did not provide guidance on how to achieve this balance, except by stating that delisting should not occur if “the interference with [an individual’s] fundamental rights is justified by [public interest]”,\textsuperscript{100} and that Google must “have regard to all the circumstances of the

\textsuperscript{95} At 110.
\textsuperscript{98} “Internet Scholars’ Open Letter”, above n 91.
\textsuperscript{99} Being irrelevance and a lack of public interest — see Part IV, “The Google Spain Right to be Forgotten”.
\textsuperscript{100} Google Spain, above n 9, at [99].
In other words, whether an individual qualifies as a “public figure” having a “public life” is left solely up to Google and its employees tasked with implementing Google Spain. This is unacceptably vague and subjective.

In response to the judgment, Google assembled an Advisory Council of unpaid independent experts who held public consultations across Europe between September and November 2014 to produce a report to help Google with compliance. The Advisory Council identified four key elements to consider in evaluating whether delisting should take place:

1. the data subject’s role in public life;
2. the nature of the information;
3. the information’s source; and
4. time.

1 Data Subject’s Role in Public Life

The Advisory Council believed that the first step is to balance “the data subject’s data protection rights and the public’s interest in access to information via a name-based search”. Although not determinative, the Advisory Council identified a spectrum of publicity to help evaluate delisting requests. The three main categories it identified were:

1. individuals with clear roles in public life;
2. individuals with a limited or context-specific role in public life; and
3. individuals with no discernible role in public life.

The level of exposure to public life corresponds with the likelihood of an individual’s delisting request being granted. At one end of the spectrum are individuals with “clear roles in public life”. This category would include those such as “politicians, CEOs, celebrities, religious leaders, sports stars, [and] performing artists”. Such roles are “less likely to justify delisting” due to the public’s “overriding interest”.

---

101 At [94].
104 At [4.1].
105 At [4.1].
106 At [4.1].
107 At [4.1].
In the middle are individuals with “a limited or context-specific role in public life”, including people such as.\footnote{108 At [4.1].}

… 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.

The content of any URLs these individuals request to be delisted will likely “weigh more heavily” than their public role(s), as delisting affects all contexts — not just those related to their role(s).\footnote{109 At [4.1].}

At the other end of the spectrum are individuals with “no discernible role in public life”. This categorisation is the most “likely to justify delisting”.\footnote{110 At [4.1].}

2 Nature of the Information

The Advisory Council identified two types of information: that with a “bias toward[s] an individual’s strong privacy interest”,\footnote{111 At [4.2.1].} and that with a “bias toward[s] a public interest”.\footnote{112 At [4.2.2].} Information with a strong argument for privacy includes:\footnote{113 At [4.2.1].}

\begin{enumerate}
\item Information related to an individual’s intimate or sex life.
\item Personal financial information.
\item Private contact or identification information.
\item Information deemed sensitive under EU Data Protection law.
\item Private information about minors.
\item Information that is false, makes an inaccurate association or puts the data subject at risk of harm.
\item Information that may heighten the data subject’s privacy interests because it appears in image or video form.
\end{enumerate}

While these factors are uncontroversial, there are certain types of information within these categories that ought to have guaranteed legal protection, such as bank account details or credit card information.
Generally, information relating to an individual’s intimate life will have “increased weight” for privacy rights. But if an individual leads a very public life, there may be public interest that justifies access to this information. With regard to financial information, public employees’ salaries or “stock holdings in public companies” may trigger public interest, or there may be “valid journalistic concerns”, especially in “investigations of corruption”.

Information that the Advisory Council found would support a decision to reject delisting due to public interest includes:

(1) Information relevant to political discourse, citizen engagement or governance.

(2) Information relevant to religious or philosophical discourse.

(3) Information that relates to public health and consumer protection.

(4) Information related to criminal activity.

(5) Information that contributes to a debate on a matter of general interest.

(6) Information that is factual and true.

(7) Information integral to the historical record.

(8) Information integral to scientific inquiry or artistic expression.

These information categories are more difficult to assess as they are more subjective. For example, under the first category, the Advisory Council believes that political discourse is “strongly in the public interest” and “should rarely be delisted”. However, if someone had an extreme political view in his or her youth, this would be exactly the type of information that may cause embarrassment later in life and lead to a delisting request.

One of the most difficult categories to determine whether to delist is information regarding criminal activity. Whether it is the victim or perpetrator of a crime that is seeking delisting will weigh in the evaluation. Legislative instruments in the EU will also affect this. For example, the Rehabilitation of Offenders Act 1974 (UK)
provides that a conviction becomes “spent” after a period of time. Nevertheless, views on past criminal activity are ultimately subjective, and vary between different cultures.

Interestingly, the Advisory Council reported that “[f]actual and truthful information that puts no one at risk of harm will weigh against delisting”. This runs counter to the CJEU’s statement that information of a prejudicial nature is not a requirement for delisting. Another problematic information category is “artistic expression”. The Advisory Council advised that an “artistic parody” of the data subject will give weight to public interest. But distinguishing between legitimate “artistic parody” and mere inflammatory acts by an internet troll again involves a subjective assessment.

3 Information Source

The source of information is relevant when evaluating a request for delisting, because not all sources operate to journalistic standards or hold the same credibility. For example, “journalistic entities” or “[g]overnment publications” would weigh in favour of public interest, as would “individual authors of good reputation”. If the publication had occurred with the data subject’s consent this would also “weigh against delisting”. In particular, Cecilia Alvarez advocated that information that data subjects uploaded themselves ought to be evaluated differently.

Google’s Transparency Report shows that the top ten websites for which delisting requests were made account for eight per cent of delisting requests. None of these top ten websites is of a journalistic nature. The website with the most removed URLs is Facebook, accounting for 14,524 removals. These statistics may help to cast a picture of the type of content and sources that attract delisting

119 As mentioned by Eric Schmidt, speaking to the Advisory Council to Google on the Right to be Forgotten (London, 16 October 2014).
120 “Advisory Council Report”, above n 96, at [4.2.2].
121 Google Spain, above n 9, at [96].
122 “Advisory Council Report”, above n 96, at [4.2.2].
124 “Advisory Council Report”, above n 96, at [4.3].
125 At [4.3].
126 At [4.3].
127 Cecilia Alvarez, speaking to the Advisory Council to Google on the Right to be Forgotten (Madrid, 9 September 2014). Alvarez discussed this in the context of “the right to regret”, where users do not foresee the consequences of uploading information about themselves.
129 Transparency Report, above n 128, as at 10 October 2016.
requests. Prima facie, the statistics undermine the criticisms based on “censorship of the media”. Simultaneously, the statistics also underline the philosophical and moral issues which underlie Google’s burden to comply with *Google Spain*, and whether Google is the “correct organ for people who are ... cleaning up their personal brand online”. However, the statistics alone are insufficient to discern whether the content delisted from Facebook is:

1. information the data subject posted about himself or herself (of which he or she may delete, but cannot delete any shared copies);
2. information posted by third parties with consent;
3. information posted by third parties with consent but later shared by other parties without consent; or
4. information posted by third parties without consent.

The possibilities for the sources of information and the degrees of consent are endless. Without more transparency from Google, it is impossible to discern whether there is overreach or conservatism in delisting decisions and whether this has resulted in the “low appeal rates”.

4 Time

The passing of time may affect the relevance and accuracy of information — the basis of Mr Costeja González’s case. The element of time and how it affects the relevance of information will vary, depending on the other criteria. For example, the “severity of a crime” will be weighed differently depending on how much time has passed. A “minor crime” committed a long time ago in a data subject’s youth may weigh in favour of delisting, while a “crime of sexual violence” may be of public interest, as the individual may seek jobs that involve “entering private homes”.

Time must also be considered in conjunction with the individual’s “role in public life”. But this, too, is problematic. Consider an individual who has been the principal of a large prestigious school for one year before retiring to seek a private life. Would there be greater or lesser public interest in this individual’s life?

---

130 Moran, above n 79.
131 “Internet Scholars’ Open Letter”, above n 91.
133 At [4.4].
134 At [4.4].
than in the life of someone who served as principal of a small, lesser-known school for several years?

Other Issues

While the Advisory Council’s Report provides an invaluable blueprint for Google to follow, it is difficult to prescribe a solution for every possible scenario. Thus, it is up to the employees at Google to manually — and arguably arbitrarily — decide this. The judgment does not stipulate that the delisting requests must be determined by a lawyer or even an employee with a legal background.

Other issues of impracticality and inconsistency exist that are too numerous to list. A key example would be that the Google Spain framework is not “future-proof”. As mentioned in Part II, humans are dynamic beings. Even if an uncontroversial delisting was granted based on an individual’s lack of “role in public life”, the individual may not always remain a “private citizen”. It may seem harmless to delist, say, teenage drink-driving records of a 25-year-old woman working at the supermarket. But would the request still be accepted if this woman happened to be dating a politician who is campaigning to lower the legal alcohol limit for driving? Worse, a superficially benign delisting request may amount to active covering up of actions that may collectively become of “public interest” if taken in the context of previous and future actions.

The crux of the balancing test involves assessing the data’s relevance given “all the circumstances of the case”, yet there are no clear criteria for either.135 The House of Lords European Union Committee has lamented that it is “wrong in principle” to order Google to evaluate thousands of “individual cases against [vague] criteria”.136 A data subject may not think that a piece of information is “relevant”, but someone seeking this information may think it is.137 As James Grimmelmann argued, “Google … provides an enormously significant online service”, but “[w]hen that service raises legal questions, we should ask whether it is good … or bad for the users.”138 The dilemma is “who are the ‘users’”? The data subjects — using Google to curate their reputation — or the searchers?

The wholesale delisting emanating from Google Spain is also problematic as delisting is the end of the road. There is no process to

135 Google Spain, above n 9, at [94].
137 Gabrielle Guillemin, speaking to the Advisory Council to Google on the Right to be Forgotten (London, 16 October 2014).
“double-check” Google’s decisions, nor any procedure to follow if delisted individuals later attract public interest. As Google has admitted, it “cannot have all the background and all the facts”.

For completeness, it is also worth mentioning that even after delisting, the “connection between the data subject and the published information” may remain intact in “Google’s backup files”. Like the territoriality issues, this is another incidence of the disconnect between the legal and technical realities. This gap between Google Spain’s goals and reality can be exploited through the use of cached pages.

The CJEU ignored the financial impact that Google Spain may have on companies in the future. Thrusting the economic and logistical burden upon search engines can have a chilling effect on small to medium enterprises and start-ups. The compliance costs would be prohibitive and could have a real effect in stifling innovation.

Although largely beyond the scope of this article, many issues arise out of the requirement that search engines evaluate delisting requests internally. The status quo is unsustainable as different search engines may reach different conclusions regarding the same delisting request. Further, it is inefficient to require data subjects to apply separately to each search engine for delisting.

Summary

Google Spain is a commendable effort by the CJEU to give some power back to individuals regarding their reputations and personal data online. However, this has been done hastily at the expense of practicality and obscures the vision of a more permanently viable solution. While the CJEU did not “fold to practical concerns”, it did choose to take a shortcut, further blurring the lines between privacy and data protection.

Google Spain has tried to humanise search engine results in a way that companies like Google do not. Google has still not acknowledged the significance of the first page of search results when

---

140 David Jordan, speaking to the Advisory Council to Google on the Right to be Forgotten (London, 16 October 2014).
141 Rustad and Kulevska, above n 6, at 365.
142 Google Spain, above n 9, at [97].
143 House of Lords Report, above n 136, at [43].
145 Powles, above n 64.
a person’s name is queried — especially by strangers.\textsuperscript{146} Nevertheless, the threshold for initiating a delisting request is too low: \textsuperscript{147} “mere embarrassment” should not be sufficient to trigger a delisting request.\textsuperscript{148} Further, even though Google has rejected 56.8 per cent of the 1,717,714 URLs evaluated,\textsuperscript{149} the fact that Google is the sole decision-maker in implementing Google Spain is inconsistent with the rule of law as the decisions lack legal certainty, consistency and transparency.\textsuperscript{150} But Google is not solely to blame for this lack of transparency, as it would breach data protection laws by divulging information regarding requests.

Ultimately, Google is an inappropriate entity for making delisting decisions. It is not independent or impartial. It has burdensome financial interests at stake. The hefty cost of compliance is plainly reflected in the extraordinary number of delisting requests Google continues to receive.\textsuperscript{151} Google Spain is a precarious solution to the problems surrounding the privacy of personal data on the web — problems which will only continue to grow worldwide.

\section*{VI THE GDPR}

The GDPR aims to modernise data protection in light of technological advances that have developed since 1995.\textsuperscript{152} It entered into force on 24 May 2016 and will apply from 2018.\textsuperscript{153}

\textbf{Article 17}

Article 17(1) provides:\textsuperscript{154}

\begin{quote}
The data subject shall have the right to obtain from the controller the erasure of personal data … without undue delay and the
\end{quote}

\textsuperscript{147} Patrick van Eecke, speaking to the Advisory Council to Google on the Right to be Forgotten (Brussels, 4 November 2014); and Bertrand de la Chapelle, speaking to the Advisory Council to Google on the Right to be Forgotten (Paris, 25 September 2014).
\textsuperscript{148} Gabrielle Guillemin, speaking to the Advisory Council to Google on the Right to be Forgotten (London, 16 October 2014).
\textsuperscript{149} Transparency Report, above n 128, as at 10 October 2016.
\textsuperscript{150} Liddicoat, above n 37 at 9.
\textsuperscript{151} Transparency Report, above n 128.
\textsuperscript{152} Rustad and Kulevska, above n 6, at 366.
\textsuperscript{153} “Reform of EU data protection rules” (12 July 2016) European Commission: Justice <http://ec.europa.eu/justice>. Note that the GDPR as adopted is significantly different from the proposed GDPR released on 18 December 2015. The few “improvements” made prior to adoption are cold comfort. For analysis of the GDPR as at December 2015, see Amanda Cheng “Let’s Forget About the Right to be Forgotten: How About a Right to be Different?” (LLB(Hons) Dissertation, University of Auckland, 2016) at 36–41; and Olivia Whitcroft “Privacy Impact Assessments and the GDPR” (2016) 26(6) SCL 6.
\textsuperscript{154} GDPR, above n 33, art 17(1).
controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent … and where there is no other legal ground for the processing;
(c) the data subject objects to the processing of personal data …
(d) the personal data have been unlawfully processed;

“Personal data”, “data subject”, data “controller” and data “processor” have almost identical definitions as in the Directive.\textsuperscript{155} These clauses prescribe stringent responsibilities for the data controller. It only takes one of the factors to trigger the right to erasure. Once triggered, the controller must “erase personal data without delay”,\textsuperscript{156} except to the extent that processing is necessary:\textsuperscript{157}

(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation … or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health …
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes …; or
(e) for the establishment, exercise or defence of legal claims.

The data subject’s rights are balanced against the right to freedom of expression in art 85. Article 85 states that Member States must make “exemptions or derogations” to “reconcile” the protection of personal data with “the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression”.\textsuperscript{158}

Article 17 extends the right to be forgotten into a right to be erased, amplifying Google Spain’s flaws. The broad language means that the scope of this right to erasure could be enforced against any number of data controllers, rather than just search engines. Although art 17 appears more detailed than the Google Spain formulation of the right to be forgotten, it does not provide any valuable guidance on the uncertainty and subjectivity issues raised in Part V. Coupled with stronger language and greater obligations for the data controller, art 17 appears to follow the erasure concepts proposed by

\textsuperscript{155} Articles 4(1), 4(7) and 4(8). For a discussion of definitions used in the Directive, see Part III.
\textsuperscript{156} Article 17(1).
\textsuperscript{157} Article 17(3).
\textsuperscript{158} Articles 85(1) and 85(2).
Mayer-Schönberger, which favours the idea of data having a “shelf life or life expectancy”.\textsuperscript{159}

Like \textit{Google Spain}, the GDPR does not set out criteria that \textit{must} or \textit{may} be considered when balancing the data subject’s rights against freedom of expression. The GDPR therefore imposes more onerous responsibilities on data controllers, while providing less guidance than \textit{Google Spain}. This ambiguity defeats the purpose of overhauling the EU’s data protection laws. Article 17 would be more workable if it included a non-exhaustive list of considerations that the data controller must or may consider when balancing data protection and freedom of expression rights.

Article 17 does not distinguish between private and public individuals. This is a significant flaw as it means that, unlike the position under \textit{Google Spain}, a data controller arguably cannot take a data subject’s “role in public life” into account when assessing a request for erasure.

Another issue with art 17 is the fact that a search engine’s main purpose is to index and display web pages relevant to the search term. This “purpose” will never become “no longer necessary”, and so search engines will arguably always have a defence against art 17(1)(a).

Article 17(2) states that when the personal data is public, the data controller “shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested … erasure”.\textsuperscript{160} In doing so, it must take into account “available technology and the cost of implementation”.\textsuperscript{161} This raises uncertainties. Is the data controller here a publisher, such as a news outlet, or is it the search engine? Under art 4(7), the data controller could be both, or either. Unhelpfully, art 17(2) does not prescribe what “reasonable steps” are, what constitutes “technical measures” nor how to balance the “cost of implementation” with the burden.\textsuperscript{162} Would data controllers who are financially less powerful be subject to less responsibility than global conglomerates such as Google?

If a data subject sought erasure from a newspaper’s website, art 17(2) means the newspaper is responsible for informing search engines of the request. Further, this could mean that the newspaper is obliged to inform innumerable other data controllers. Alternatively, if the data subject sought erasure from a search engine directly, the

\textsuperscript{159} Mayer-Schönberger, above n 48, as cited in Rustad and Kulevska, above n 6, at 383–384.
\textsuperscript{160} Article 17(2).
\textsuperscript{161} Article 17(2).
\textsuperscript{162} Article 17(2).
search engine would have to inform the newspaper of such a request, as well as other search engines and innumerable data controllers.

If art 17 is interpreted as above, in a Google Spain scenario, online publishers could face serious issues when presented with a delisting request, as they would now need to:

1. defend the “purposes” for which personal data was collected or processed — such as public interest — as still necessary under art 17(1)(a);
2. inform third parties, including search engines or social media outlets sharing the relevant URL, of erasure requests; and
3. as a last resort, defend its freedom of expression as a counterargument to justify keeping the information online, under arts 17(3)(a) and 85.

Although this interpretation is unintended, ambiguity that leaves such an interpretation available is extremely problematic. The GDPR opens the floodgates to onerous consequences and responsibilities for news providers. A more pragmatic solution is required to balance individuals’ rights against online dissemination of information.

Tangentially, art 18 outlines situations where data shall be processed in a restricted manner, rather than erased. This conforms to the theory that the right to be forgotten should give the data subject one of three rights:

1. the right to have information deleted after a preset period;
2. the right to have a clean slate; and
3. the right to be connected to current information and delinked from outdated information.

For example, if a data subject contests the data’s accuracy, art 18(1)(a) instructs the data controller to restrict processing the data for a period of time to verify the data’s accuracy.

**Article 35**

Article 35 requires the data controller to carry out a data protection impact assessment (DPIA) where processing is “likely to result in a high risk to the rights and freedoms of natural persons” due to the “nature, scope, context and purposes of the processing”. The DPIA

163 Article 18.
164 Rustad and Kulevska, above n 6, at 367.
165 Article 35(1). While this is a higher threshold required to trigger the DPIA obligations when compared with art 33 in the December 2015 iteration of the GDPR, the author believes the threshold is still too low. See Cheng, above n 153, at 40–41.
requires a report on the “safeguards, security measures and mechanisms” ensuring personal data protection,\textsuperscript{166} and goes so far as to require the controller to “seek the views of data subjects … on the intended processing”.\textsuperscript{167} Article 35(3) identifies types of processing operations that would particularly require a DPIA.

The GDPR does not explicitly stipulate that art 35 will apply to the data processing conducted by search engines. However, an art 35 DPIA will be likely required because:

\begin{enumerate}
  \item search engines process a large, ever-expanding scope of data;\textsuperscript{168}
  \item data relating to “personal aspects” is processed in an "extensive", "automated" manner and could significantly affect the person;\textsuperscript{169} and
  \item search engines function by "systematic[ally] monitoring … a publicly accessible area on a large scale".\textsuperscript{170}
\end{enumerate}

Article 35’s various requirements create difficulty in ascertaining a search engine’s obligations as a data controller. The nature of a search engine’s processing falls easily within the ambit of requiring a DPIA. However, a DPIA’s required steps are incompatible with the activity undertaken by a search engine. It would be completely unfeasible for Google to seek the views of all the data subjects included in its search results.

\textbf{Further Comments}

Interestingly, unlike the Directive, the GDPR does not use the terms “inadequate, irrelevant or no longer relevant, or excessive”. If Google \textit{Spain} had arisen under the GDPR, art 6(1)(e) could be interpreted to deny Mr Costeja González’s delisting request. As the \textit{La Vanguardia} articles were statutorily ordered, it would be open for the court to interpret both the publisher and search engine to be processing such data for the “exercise of official authority”, which would be lawful.\textsuperscript{171}

The GDPR’s purpose is to modernise and align data protection law with today’s technological realities. It is unacceptable that such an extensive reform is ambiguous in wide-reaching clauses. This uncertainty only muddies the already murky waters that search

\begin{footnotes}
\textsuperscript{166} Article 35(7)(d).
\textsuperscript{167} Article 35(9).
\textsuperscript{168} Article 35(1).
\textsuperscript{169} Article 35(3)(a).
\textsuperscript{170} Article 35(3)(c).
\textsuperscript{171} Article 6(1)(e).
\end{footnotes}
engines are treading in the wake of Google Spain. Further, the ill-defined boundaries of arts 17 and 35 problematically impose rigorous obligations on the data controller.

It is outside this article’s scope, but the legal concepts of “data controller” and “data processor” need to be redefined. As mentioned, the CJEU was unable to create a legal category more pertinent for search engines. But the GDPR would have been an appropriate forum to reconceptualise the role of search engines, and clarify search engines’ data protection obligations.

Ultimately, the GDPR is unhelpful in the search for a better solution to the “very real problem” that Google Spain tried to resolve.  

VII AN ALTERNATIVE SOLUTION: THE RIGHT TO BE DIFFERENT

Taking heed of Google Spain and the GDPR’s pitfalls, this article proposes an alternative solution. Instead of focusing on erasing past, out-of-date, or “irrelevant” information from search engines, the solution should, prima facie, be to add or update the information. Important core aims must be kept in mind. The solution ought to be one that will be accepted globally, will not risk undermining freedom of expression, and will be viable in a permanent or at least long-term time frame.

First, it is important to identify the underlying reason that Mr Costeja González and the 1.7 million people in the EU wish to have their information “forgotten” by Google. The reason is not that the information is false. Rather, those who wish to be “forgotten” feel they are “not that person anymore”. These individuals wish to be different from their previous selves, and want their online search results to reflect who they feel they currently are, not who they used to be. This can be framed as a “right to be different from oneself”.  

Secondly, any solution must address the main criticisms surrounding Google Spain and the GDPR’s right to be forgotten, which is that these laws encroach on freedom of expression without independent oversight.

172 Zittrain, above n 5.
173 Transparency Report, above n 128, as at 10 October 2016.
174 de Andrade, above n 7.
Thirdly, it is undesirable for the web to become Balkanised in such a way that people in different geographical locations have access to different information.\textsuperscript{175}

This article proposes a long-term solution that combines delisting and contextualisation — also known as a “right of reply”. Identity is a “cultural and social construct” that is constantly in flux as we “choose” who we want to be.\textsuperscript{176} Identity can also be conceptualised as a narrative that “can be constantly revised and changed”.\textsuperscript{177} If individuals are able to “modify names, drop nationalities and change sex”, they should also be able to alter the representation of their identity on the web.\textsuperscript{178}

Powles proposed that data subjects should be given a “right to reply” in the form of tagging search results.\textsuperscript{179} When a right of reply has been exercised, a searcher may click on a link beneath the search result in order to read information that has been lodged in response to the information in the search result.\textsuperscript{180} The purpose and merit of contextualisation rather than delisting is that the original information remains online. It is true that allowing the original information to remain online could still prejudicially affect the data subject. However, if ordinary members of society on a jury are entrusted to weigh up competing evidence and ascribe appropriate weight to each element, then the general public should also be entrusted and given the chance to do the same with information on the web. Contextualisation is less controversial as it does not provoke any freedom of expression or censorship criticisms.

Ultimately, this is not a strictly legal privacy or data protection issue. This is a very human problem about identity and change. Instead of aiming to be forgotten — which collides with the public’s right to information and to remember — the proposed solution aims to recognise a right to be different.

**Mechanics of the Solution**

Contextualisation should be the starting point and default solution. Delisting should only occur in exceptional circumstances. Giving an individual complete control over his or her identity is “undesirable” and “impossible”.\textsuperscript{181} As such, contextualisation allows the data subject’s freedom of expression to challenge and offset the publisher’s

\textsuperscript{175} Jeffrey Toobin “The Solace of Oblivion” *The New Yorker* (online ed, New York, 29 September 2014).
\textsuperscript{176} de Andrade, above n 7, at 129.
\textsuperscript{177} At 129.
\textsuperscript{178} At 129.
\textsuperscript{179} Powles, above n 64.
\textsuperscript{180} Powles, above n 64.
\textsuperscript{181} de Andrade, above n 7, at 130.
allegedly inaccurate or irrelevant exercise of his or her freedom of expression.

Both contextualisation and delisting requests would require the data subject to provide evidence verifying the truthfulness of his or her “reply”, or reason for requesting delisting. Permanence is the ultimate goal. Not every request necessitates a remedy. The deciding test for whether a data subject should be granted contextualisation or delisting is: does this piece of information alter the narrative, either of the event or the data subject’s life? If answered in the affirmative, then only contextualisation may be considered. If, in contrast, the data does not alter the narrative, then both delisting and contextualisation may be considered. In other words, the decision must be timeless, such that the solution would remain the same if the request for delisting or contextualisation were lodged at any point in the future. It is envisaged that very few delisting requests would pass this test — instead, contextualisation could be granted as a compromise, or nothing at all.

For example, delisting a convicted criminal’s crimes would alter his or her life’s narrative. Conversely, a right of reply allows elaboration on how he or she is now different, such as: the crime was committed X years ago; he or she has paid $Y in reparations to the victim; and has served Z time in prison. The data subject may also wish to add that he or she has since been working at ABC company for D length of time and contributes actively to society by volunteering at EFG charity. This way, all information on the search results page would be accurate, without either the publisher or data subject’s fundamental rights being quashed in favour of the other. Both parties get a compromised version of what they want; publishers can disseminate the information, while data subjects can reduce the harm to public perceptions of them.

A victim of crime, in contrast, should be granted delisting so that an article outlining the crime is not associated with searches for his or her name. It is in no one’s interests that an innocent person unto whom harm was done is forever remembered as “the person that bad thing happened to”. Another example where delisting should be granted is if an irrelevant third party commented on an incident, without expressing any strong personal opinions or views. For example, if F’s neighbour’s house was burgled and F told a reporter that he or she called the police after hearing a burglar alarm, F should be granted delisting of an article containing such facts. However, if F expressed strong personal opinions or views, such as using offensive racist slurs in the interview, the article should not be delisted. This is because the narrative of F’s life is altered by the taint of comments.
The default position should be to *add* rather than remove information. Although an individual’s “role in public life” ought to be taken into account, it is expected in this modern age that everyone is “Google-able”, and as such, have some element of a “public life”. Since the default is to add information and retain the narrative, the “public figure” element would not feature as strongly in this solution, unlike the *Google Spain* test. The suggested starting point for a formula is therefore as follows:

(1) If the individual is the main subject of, or heavily influences the narrative, then only a right of reply should be granted.

(2) If, however, the individual’s contribution to the information is only incidental (such as a witness to a crime who merely recounts events and does not express personal opinion), then delisting may be offered as it does not detract from the narrative.

(3) Nevertheless, without a good reason justifying delisting, a right of rely — and not delisting — should be granted. Mere embarrassment from a thoughtless comment or act would not usually suffice for delisting to take place. In these cases, the data subject may apologise for the comment, or merely note that some time has passed and he or she no longer holds such views.

(4) Victims of crime should prima facie have all identifying features removed and delisted.

This article recommends an independent quasi-judicial body be set up to deal with such requests. This would serve the purposes of promoting transparency, accountability and consistency, which are the main concerns associated with Google evaluating delisting requests in-house as per *Google Spain*. For example, this independent body could issue a decision and specify the “reply” to be implemented on search results across all search engines. This means the outcome is consistent across all search engines and the data subject would not have to apply to different companies to exercise this right. However, even in the absence of such an independent body, the right to be different would still provide a better solution than *Google Spain* and the GDPR.
The social and legal issues raised in this article are difficult to reconcile. This is exacerbated by the web’s trans-jurisdictional nature. Although the Directive, Google Spain and the GDPR are admirable efforts by the EU to give individuals more power over their personal data, the practical result is contrived and undesirable. Privacy and data protection are not neatly distinct. Still, the two concepts should not be confused in our search for autonomy over individual reputation and identity on the web.

This article’s proposed solution — a right to be different — is merely a starting point, intended to provoke a change in direction of the legal discourse. We cannot continue to apply stringent concepts of “data controllers” which are over two decades old. It is 2016. Our world is full of new technology and uses for that technology which could barely be imagined when the Directive was enacted. The GDPR does not address this adequately.

The right to be different urges policy and law makers to rethink enacting legal instruments that have far-reaching effects both in geography and time. Any solution intended to protect individuals or “data subjects” ought to consider the lasting effects that altering an index of information will have. Just because a piece of information may not seem to be of “public interest” now does not mean it will always remain that way. Humans are not static beings. That fact is the core and the cause of the problem at hand, and accordingly must be central in its solution. But permanence is important too: the narrative of events and of a person’s life should not be so easily changed in search engine results.

Google is aware of how powerful its search results are in uncovering people’s personal details. Job applicants and employers are also aware of this. However, a “cognitive adjustment” is likely to occur over time as the ubiquity of the web in everyday life continues. Social norms and expectations will change. People will become increasingly desensitised to prejudicial or unfavourable information regarding others on search engine results as they realise that they, too, have a trail of changed identities and behaviours documented online.

182 For example, Google blacklisted CNET reporters after they published an article revealing personal information regarding Google CEO Eric Schmidt. All the personal information published was uncovered from Google search results. See Richard Esguerra “Google CEO Eric Schmidt Dismisses the Importance of Privacy” (10 December 2009) Electronic Frontier Foundation <www.eff.org>; and Jennifer Westhoven “CNET: We’ve been blackballed by Google” (5 August 2005) CNN Money <money.cnn.com>.

183 Rustad and Kulevska, above n 6, at 385.