THE BEST PRACTICE OF FORGETTING

ABSTRACT

Examining the ‘right to be forgotten’ in the European Union (EU) in the aftermath of the Google Spain v. AEPD and Mario Costeja Gonzalez decision, this Comment argues the need for a Centralized Data Protection Agency. In May of 2014, the Court of Justice of the European Union determined in Costeja that citizens of EU member states have the right to ask search engine companies to remove certain personal information from search results. Search engine companies, viewed by the court as ‘data controllers’, are required to consider the takedown requests in light of the individual’s privacy rights, but are not required to remove the requested information if the company determines that those privacy rights are outweighed by the public’s interest in the information. The European Commission later issued guidelines on the Costeja decision, adding the provision that if a request is rejected, the citizen may appeal to their local court or Data Protection Agency. This Comment argues that the lack of specific guidance in the Costeja decision ultimately created significant burdens on citizens, Internet search engine companies, and the EU member states. To mitigate these burdens, a Centralized Data Protection Agency, as this Comment envisions, would receive requests directly from citizens, weigh the privacy versus public interest rights, and make decisions that would be binding across all member states. The creation of an EU-wide organization would streamline the takedown request process by providing all citizens with a single authority to which they could submit requests. This solution would make the request process easier for citizens, relieve private search engine companies from the daunting responsibility of determining legal privacy rights, and insulate member states from conflicting local implementation.
INTRODUCTION

Most things are forgotten over time. Even the war itself, the life-and-death struggle people went through, is now like something from the distant past. We’re so caught up in our everyday lives that events of the past, like ancient stars that have burned out, are no longer in orbit around our minds. There are just too many things we have to think about every day, too many new things we have to learn. New styles, new information, new technology, new terminology . . . But still, no matter how much time passes, no matter what takes place in the interim, there are some things we can never assign to oblivion, memories we can never rub away. They remain with us forever, like a touchstone.

—Haruki Murakami

In 2014, the “right to be forgotten” suddenly transformed from an amorphous concept set forth by the European Union (EU) in its series of privacy directives from 1995 into an operative pan-European law with the decision by the Court of Justice of the European Union to honor the request of Mario Costeja González, an ordinary individual with credit problems in his past, to have news articles pertaining to him omitted from Google’s search results. In the aftermath of this decision, Google received hundreds of thousands of requests from citizens wishing to have information about them hidden. The requirements imposed on Internet intermediaries by the Court of Justice of the European Union in the Google v. Costeja opinion and subsequent guidelines issued by the European Commission have proven to be cumbersome for citizens wishing to exercise their ‘right to be forgotten,’ overwhelming for Internet intermediaries, and distressing for local governments. This paper critically examines these problems and suggests that a centralized data protection agency would provide solutions by creating a streamlined process for information removal requests.

On the first day of compliance with the Costeja opinion, Google received more than 12,000 takedown requests. In response to subsequent rejections of

---

requests for information to be removed from search results, citizens appealed
the rejections in the courts of their home jurisdictions. Google itself has
expressed concerns as to the scope of responsibility and challenges of
implementing a coherent method to comply with the Costeja opinion. The
European Commission has revealed that it expects Google and other search
engines to implement takedown requests globally, not exclusive to search
results within the EU. Some EU Member States have raised doubts and
questions of their own in regards to the practicality and legitimacy of giving
search engines the principal authority in the implementation of the new ‘right
to be forgotten’ policy.

This Comment reveals a disconnect between the EU’s promise of a ‘right to
be forgotten’ and the execution of an effective method for implementing this
revolutionary policy. It shows how the current implementation method
undermines the ability of citizens to control access to personal information in a
meaningful way. It then demonstrates how a centralized agency may be better
qualified than individual Internet intermediaries to manage and minimize these
problems, thus allowing citizens to more effectively exercise their right to
privacy on the Internet.

I. THE COSTEJA DECISION AND IMPLEMENTATION

What should concern us is not that we can’t take what we read on the
internet on trust—of course you can’t, it’s just people talking—but
that we ever got into the dangerous habit of believing what we read

5 See Natasha Lomas, Europe Seeks a Common Appeals Process for the ‘Right To Be Forgotten’,
Court of Justice of the European Union, Judgment in Joined Cases C-509/09 and C-161/10 (Oct. 25, 2011)
[hereinafter Court of Justice Press Release] (concluding that “[v]ictims of infringements of personality rights
by means of the internet may bring actions before the courts of the Member State in which they reside in
respect of all of the damage caused”).

6 Letter from Peter Fleischer, Global Privacy Counsel, Google, to Isabelle Falque-Pierrotin, Chair,

7 Article 29 Data Protection Working Party, Guidelines on the Implementation of the Court of Justice of
the European Union Judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos
(AEPD) and Mario Costeja González” C-131/12, EUROPEAN COMMISSION, at 3 (adopted on Nov. 26, 2014),

8 SUB-COMMITTEE ON HOME AFFAIRS, HEALTH & EDUCATION, REPORT, 2014-15, HL 40, ¶ 36 (UK)
[hereinafter UK SUB-COMMITTEE REPORT]; Stephanie Bodoni, EU Seeks to Curb Google Control of Right to
seeks-to-curb-google-control-of-right-to-be-forgotten.
in the newspapers or saw on the TV—a mistake that no one who has met an actual journalist would ever make.

—Douglas Adams

What happens when old, irrelevant information on the Internet begins to affect your personal life? What is the remedy when a mistake in your past comes back to haunt you? This is exactly what happened to Mario Costeja González, a citizen of Spain. In 2009, a search for Mr. Costeja’s name on Google, the world’s leading search engine with a vast market-share, returned Spanish newspaper articles from 1998 announcing that Mr. Costeja’s home had been repossessed and would be auctioned off to satisfy tax debt he owed to the government. Although these announcements were true and factual at the time of their publication, Mr. Costeja had paid off the debt long before 2009, and the ultimate purpose of the articles to attract bidders to the auction of his property was no longer relevant. In an era when searching for someone on the Internet is a frequently employed tool for vetting his or her integrity, Mr. Costeja sought to have the old and irrelevant information removed from the website to avoid any potential damage to his reputation in the future.

A. Mario Costeja González’s Complaint and Trials

During 1998, two separate notices appeared in a Catalan newspaper, La Vanguardia, announcing that Spanish national Mario Costeja González was a party to “a real-estate auction connected with attachment proceedings for the recovery of social security debts.” The notices later appeared on the newspaper’s Internet website, accessible to persons in all parts of the world.

9 How to Stop Worrying and Learn to Love the Internet, SUNDAY TIMES (Aug. 29, 1999), http://www.douglasadams.com/dna/19990901-00-a.html.
13 See id.
with unrestricted Internet access. Mr. Costeja filed a complaint on March 5, 2010, with the Agencia Española de Protección de Datos (AEPD), requesting the information on La Vanguardia’s website to either be removed altogether or alternatively modified in a way that the websites containing the information about him would be hidden from the inquiries of Internet search engines because “the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant.” He further asked for Google to directly exclude all links from its search results that referred to this particular personal information about himself, in addition to the specific links to those pages of La Vanguardia.

The AEPD subsequently rejected the first part of Mr. Costeja’s request for the newspaper to either take down the information or alter the website to make it less visible to search engines because “the information in question was legally justified as it took place upon order of the Ministry of Labour and Social Affairs and was intended to give maximum publicity to the auction in order to secure as many bidders as possible.” Nevertheless, the AEPD upheld Mr. Costeja’s request for Google to omit all websites containing or linking to the information in dispute. The AEPD found Google and other search engines to have a responsibility “as intermediaries in the information society” because they ultimately allow the information to be disseminated and located by the public. These activities were held by the AEPD to be subject to the “fundamental right to data protection and the dignity of persons” and therefore search engines should comply with the requests of individuals to make personal data unavailable via hiding certain search results from third parties.

The Audiencia Nacional (National High Court of Spain) determined that individuals could request search engines to hide third party websites containing personal information if the requests fell within the context of the EU’s 1995

**B. Ruling by the Court of Justice of the European Union**

The Court of Justice of the European Union (the Court) first determined that under the 1995 Data Protection Directive Section 46 (Directive 95/46), Internet search engine providers such as Google are data ‘controllers’ of information and personal data. As controllers, search engine operators are obligated to remove links to third party websites containing certain information that identifies an individual by name, even when the law protects the third party from having to remove the information being displayed on the hosted website.

The *Costeja* opinion lays out the broader rule that citizens of Member States may request to have personal information hidden by search engines as data controllers when the information is essentially superfluous:

> [I]f it is found . . . that information appears, having regard to all the circumstances of the case, to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing at issue carried out by the operator of the search engine, the information and links concerned in the list of results must be erased.

This rule requires search engines as data controllers to examine each request and take into consideration “a balancing of the opposing rights and interests concerned” to ensure that the right of the citizen is greater than the “interest of the general public in having . . . access to the information in question.” In the event that the data controller ultimately rejects the request, the citizen then “may bring the matter before the supervisory authority or the judicial authority so that it carries out the necessary checks and orders the controller to take specific measures accordingly.”

---

24 Id. ¶ 19.  
25 Id. ¶ 20.  
26 Id. ¶¶ 33, 34, 41.  
27 Id. ¶ 62.  
28 Id. ¶ 94.  
29 Id. ¶ 74.  
30 Id. ¶ 100 n.4.  
31 Id. ¶ 77.
C. Implementation of the Court’s Holding

On the first day of compliance with the Costeja opinion, Google received more than 12,000 takedown requests. Co-founder of the search giant, Larry Page, expressed concern that this exertion of regulatory force from a government body on the Internet poses a serious threat to future Internet start-up companies, and may also impede the free flow and collection of data that holds potential to be of benefit to society. Despite the company’s apprehensions and fear of the overarching effects of the Costeja opinion, Google nonetheless has taken proactive steps in complying with the Court’s orders. The company first rolled out a webform for citizens of the EU to submit their privacy requests, requiring at least one form of government issued identification. Google also began an open and ongoing conversation with the EU about its particular concerns regarding the difficulties handling the volume of requests and performing the balancing test required by the Court. In addition, Google assembled an eight member advisory council to lobby the EU for clearer guidelines for the post-Costeja ‘Right to Be Forgotten’ (RTBF) policy.

On November 26, 2014, the Article 29 Data Protection Working Party (WP29), on behalf of the European Commission, released guidelines for the implementation of the Costeja judgment. These guidelines echoed the orders of the Court, requiring search engines as data controllers to accept RTBF takedown requests directly from citizens. If a search engine denies an RTBF

---

35 Waters, Google Bows to EU Privacy Ruling, supra note 33.
37 See Letter from Peter Fleisher, supra note 6.
39 WP29 Guidelines, supra note 7, at 7.
40 Id.
request, the citizen may then seek remedy from either his or her local official Data Protection Agency (DPA) or local judicial system. 41

Privacy experts as well as independent Member States have criticized this method of implementing the new RTBF policy because it gives companies, such as Google, the power to privately regulate speech and control access to information on the Internet at their own discretion. 42 By mid-September of 2014, only four months after the Costeja ruling, at least 193 known appeals had been filed by citizens in their local courts to dispute denied requests by Google.43 About a month later, Google revealed that it had received more than 144,000 individual requests for removal, and had subsequently granted approximately forty-two percent of the requests. 44 Overall, it appears that the EU is content to implement a revolutionary policy to protect the privacy interests of its citizens on the Internet, as long as it does not have to do the heavy lifting. 45

II. THREE KEY PROBLEMS CREATED BY THE CURRENT IMPLEMENTATION OF THE RTBF POLICY

The EU has taken a firm stand in recognizing the privacy rights of its citizens. 46 The new RTBF policy is a major step forward in ensuring the robust protection of those individual privacy rights. 47 While the road paved by the Court’s Costeja opinion is bursting with good intentions, some inevitable complications have arisen along the way. First, the current method of implementation creates substantial obstacles and potential privacy vulnerability

---

41 Where a search engine refuses such a request, the data subject may bring the matter before the DPAs, or the relevant judicial authority, so that they carry out the necessary checks and take a decision in accordance with their power in national law. Id. at 12.
42 See generally UK SUB-COMMITTEE REPORT, supra note 8; Index Blasts EU Court Ruling on “Right to be Forgotten”, INDEX ON CENSORSHIP (May 13, 2014), http://www.indexoncensorship.org/2014/05/index-blasts-eu-court-ruling-right-forgotten/.
43 See Lomas, Google Offers Webform, supra note 36; Court of Justice Press Release, supra note 5.
47 See generally id.
for citizens who wish to exercise their nationally recognized right to privacy, even when they lack the fundamental access or knowledge required to make an RTBF request. Second, implementation burdens the Internet industry by requiring private companies to handle thousands of requests from citizens, asking the companies to make difficult and important decisions that could affect individual privacy, freedom of speech, and public access to information. Third, the implementation has created a strain on local jurisdictions from unsatisfied citizens who have had their RTBF requests rejected by search engines and continue to seek remedy, occasionally resulting in inconsistent results across Member States.

A. Undue Burden on Citizens: Cumbersome Requirements to Exercise Rights and Potential Privacy Risks

At the heart of the RTBF policy is intent to protect the privacy rights of all citizens of the EU by allowing them to control public dissemination of their private information. However, the current implementation of the new RTBF policy poses multiple challenges for citizens: first, the general inability to make a request by any means other than through the Internet; second, the necessity to place a unique request to each existing search engine or data controller with the possibility that some data controllers will honor certain takedown requests that other data controllers may deny; third, the use of local jurisdictions as a final resort, where varying territories may reach differing conclusions; fourth, the private sector taking advantage of the new RTBF policy implementation by offering takedown request services to citizens that may pose significant risk for identity theft.

50 UK SUB-COMMITTEE REPORT, supra note 8.
51 Id.
52 WP29 Guidelines, supra note 7, at 12.
1. Citizens Must Submit RTBF Takedown Requests Online

The first problem facing citizens is that the RTBF takedown request forms are currently only available to submit online. Although it may seem unimaginable in the highly developed countries of the EU, in 2012 the European Commission released a report revealing that twenty-four percent of the citizens of the EU had never used the Internet. The report concluded that “[b]eyond lack of interest and of skills, equipment and access, costs are the main reasons declared by European households for not having access to the Internet.” In the United Kingdom, seventy percent of individuals without access were found to voluntarily exclude themselves from the technology, expressing indifference towards ever using the Internet. As of January 1, 2015, all major search engine companies accepting RTBF requests only accept takedown requests via the Internet. Regardless of whether a citizen has never used the Internet for voluntary or involuntary reasons, is not a frequent user, or does not have access to the Internet at home, these factors do not preclude that individual from their privacy rights as they relate to the Internet. For example, a citizen who does not have the financial means to maintain Internet service in their home may still wish to file a request to have inaccurate or irrelevant information about them removed from search inquiries. This hypothetical citizen would need to obtain, at minimum, access to a computer with Internet access, an email address for the purpose of receiving communication about their request, and a method of scanning and uploading official documented proof of their citizenship.

54 E.g., Request to Block Bing Results, supra note 49; GOOGLE, Search Removal Request, supra note 49.
56 Id. at 4.
57 Chris Tryhorn, Most People Without Internet Have No Interest In Getting Broadband, GUARDIAN (June 10, 2009, 2:23 AM), http://www.theguardian.com/media/2009/jun/10/ofcom-broadband-research.
58 See generally John Ribeiro, Bing Follows Google in Offering Europeans the ‘Right to be Forgotten’, PCWORLD (July 17, 2014, 8:36 AM), http://www.pcworld.com/article/2455240/microsofts-bing-follows-google-in-offering-europeans-the-right-to-be-forgotten.html; Request to Block Bing Results, supra note 49; GOOGLE, Search Removal Request, supra note 49.
59 “To prevent fraudulent removal requests from people impersonating others, trying to harm competitors, or improperly seeking to suppress legal information, we need to verify identity. Please attach a legible copy of a document that verifies your identity (or the identity of the person whom you are authorized to represent). A passport or other government-issued ID is not required.” GOOGLE, Search Removal Request, supra note 49.
and ultimate outcome of their request. There are many hypothetical examples
in which access to these resources may prove especially challenging: an elderly
individual; a working single parent; an individual with disabilities that does not
have convenient means of transportation or mobility; or an individual residing
in a particularly secluded region. Although the European Parliament has
emphasized the importance of free Internet access as a public resource to
disadvantaged groups via the public library system, many Member States
have increasingly cut funding to their public libraries, resulting in mass
closures that further restrict access to this critical resource.

2. Citizens Must Submit Unique Takedown Requests to Each Individual
   Data Controller

Another problem is the necessity for citizens to file different requests for
every unique search engine or data controller that exists either now or in the
future. This is especially burdensome when considering that there are
hundreds of thousands of search engines in existence, and new search engines
can appear overnight. Even after successfully completing all relevant
applications to request the removal of information, there remains the concern
that each data controller may make contradicting decisions on the same
request, resulting in the information being removed from some, but not all
sources. With this result, the only recourse left for the citizen would be to file
a complaint within their local jurisdiction, which raises a whole bundle of
separate issues regarding accessibility to the court system and feasibility of
bringing a successful suit.

---

60 To place an RTBF takedown request, Google requests a “[c]ontact email address . . . where emails
about your request will be sent.” Id.
61 Written Declaration Recognising the Essential Social Role of Public Libraries, EUROPEAN BUREAU
LIBRARY INFO. & DOCUMENTATION ASS’NS (Oct. 18, 2013), http://www.eblida.org/news/written-declaration-
AM), http://www.theguardian.com/books/2012/dec/10/uk-lost-200-libraries-2012.
63 UK SUB-COMMITTEE REPORT, supra note 8.
64 See, e.g., Ronak Desai, Qi Yang, Zonghuan Wu, Weiyi Meng & Clement Yu, Identifying Redundant
Search Engines in a Very Large Scale Metasearch Engine Context, Proceedings of the 8th Annual ACM
International Workshop on Web Information and Data Management 51 (2006); Keir Thomas, Three New
Search Engines Worth Checking Out, PCWORLD (Mar. 21, 2011, 2:47 PM), http://www.pcmag.com/article/
222727/google_alternatives_three_new_search_engines_worth_investigating.html.
65 UK SUB-COMMITTEE REPORT, supra note 8.
66 WP29 Guidelines, supra note 7, at 12.
3. Citizens May Experience Conflicting Results in Local Jurisdictions

Search engine companies are not the only players in the RTBF game who may not reach a mutual consensus. The third problem facing citizens is that the regional courts and DPAs within the Member States of the EU may differ in their individual assessments of RTBF requests on appeal. This issue of inconsistent implementation of policy among Member States “resulting in divergences in enforcement” was a major stumbling block for the EU’s 1995 Data Protection Directive,67 and these past lessons of inconsistent policy implementation must be taken into consideration.

4. Citizens May be Taken Advantage of by Private Companies, Creating Additional Privacy Risks

The final issue that may lead to complications for citizens is the fact that business entrepreneurs have been eager to take advantage of the new RTBF policy, launching companies to specifically aid citizens in the process of submitting takedown requests.68 The first known spawn of business models built on the concept of RTBF takedown services was Forget.me, a company that provides customers with assistance in completing the online request forms.69

Two particularly problematic situations arise for citizens when third party actors get involved with the RTBF takedown request process. First, citizens who pay for the help of a third party service to facilitate a request have no guarantee that it will result in a successful takedown.70 Regardless of this fact, companies will continue to take a customer’s money with little to no discretion as to whether or not the RTBF claim is actually viable.71

Second, citizens open themselves up to identity theft when they reveal personal information to third parties. A study conducted by the European Commission in 2012 confirmed a direct link between Internet usage and an increased risk of identity theft. It is possible for companies to fraudulently operate in this particular service industry as a front, with the actual motive of collecting citizen’s private information such as their email address or other valuable identifying information from the official documentation they are required to provide for the request. Even if this false-front organization does follow through with making the request, it could easily sell citizen’s sensitive information that the company has collected in the process to another third party on the black market.

Other companies that operate legitimately in this service industry also pose a threat to citizens because of the necessity to collect sensitive personal information for the request creates a risk of the company’s system being compromised or a corrupt employee surreptitiously stealing customer information. Either way, allowing a third party actor to handle sensitive information, regardless of the actor’s legitimate intent, creates another distinct threat to citizen’s privacy beyond the scope of what the RTBF policy was designed to address. The goal of the RTBF policy is to empower citizens with the ability to control the dissemination of their personal information, but the current method of implementation overall appears to give citizens more problems than power.

73 Id.
75 Id.
77 “The 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.” Myth-Busting the Court of Justice of the EU and the “Right to be Forgotten”, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_rtf_mythbusting_en.pdf (last visited Feb. 14, 2015).
B. Undue Burden on the Internet Industry: Unwelcome Power and Lack of Resources

Search engines have become a critical part of the way people use the Internet.\footnote{\textquoteright\textquoteleft\text{The two means of access to web information most often used are search engines and links or recommendations from other websites.\textquoteleft\textquoteleft} Ruud Koopmans & Ann Zimmerman, \textit{Visibility and Communication Networks on the Internet: The Role of Search Engines and Hyperlinks}, in A EUROPEAN PUBLIC SPHERE: HOW MUCH OF IT DO WE HAVE AND HOW MUCH DO WE NEED 220 (2007).} They are commonly used as the starting point for Internet browsers—in other words, it is the very first thing someone sees when they log onto the Internet. Google is often ranked by analytics trackers as the most visited website in the world.\footnote{E.g., The Top 500 Sites on the Web, ALEXA, http://www.alexa.com/topsites (last visited Jan. 11, 2014).} Due to this overwhelming popularity of use by the general public, the Court decided that search engines should be accountable as gatekeepers, responsible for administering privacy rights on the Internet.\footnote{Jo Best, \textit{The Right to be Forgotten: Can We Really Trust Google to Decide When Our Data Should Die?}, ZDNET (June 5, 2014, 9:42 AM), http://www.zdnet.com/article/the-right-to-be-forgotten-can-we-really-trust-google-to-decide-when-our-data-should-die/.} This position creates several problems: first, search engines prefer to hold themselves out as passive conduits of information, rather than active controllers;\footnote{See Jeffrey Toobin, \textit{The Solace of Oblivion: In Europe, the Right to be Forgotten Trumps the Internet}, NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion.} second, small Internet companies lack the same resources as their larger counterparts to effectively police content;\footnote{Peers Say 'Right to be Forgotten' Principle Unreasonable, BBC NEWS (July 29, 2014, 8:03 PM), http://www.bbc.com/news/uk-politics-28551845; Waters, \textit{Google Bows to EU Privacy Ruling}, supra note 33.} third, the three-steps required for the RTBF takedown process are difficult for private companies to implement, even for giants such as Google.\footnote{Sam Schechner & David Roman, \textit{Google Seeks Views in Europe on Right to be Forgotten}, WALL STREET J. (Sept. 9, 2014), http://online.wsj.com/articles/google-seeks-views-in-europe-on-right-to-be-forgotten-1410268827.}

1. Search Engines as Passive Conduits v. Active Controllers

By designating search engines as controllers of information rather than neutral intermediaries as they have held themselves out to be, the EU has put companies such as Google in a position of power that they do not desire.\footnote{See Alan Travis & Charles Arthur, \textit{EU Court Backs 'Right to be Forgotten': Google Must Amend Results on Request}, GUARDIAN (May 13, 2014, 9:06 AM), http://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results; Matthew Weaver, \textit{Google 'Learning As We Go' in Row Over Right to be Forgotten}, GUARDIAN (July 4, 2014, 5:34 AM), http://www.theguardian.com/technology/2014/jul/04/google-learning-right-to-be-forgotten.} Google’s attitude towards its defined role on the Internet is that of a passive
directory providing access to information, like a card catalog in a public library. General Counsel Kent Walker points out: “We don’t create the information. We make it accessible. A decision like this, which makes us decide what goes inside the card catalogue, forces us into a role we don’t want.” This passive stance may seem counterintuitive to features such as Google’s patented PageRank algorithm that treats links like weighted votes to determine the specific order of websites that will be displayed in search results. Despite factors such as the PageRank algorithm, search engines are treated as neutral intermediaries in the United States, and are shielded from liability for third party content when they do not directly encourage or participate in the illegal activity of the third party directly.

Regardless of its passive posturing and resistance to being labeled as a data controller, Google immediately sought to comply with the Costeja ruling. David Price, one of Google’s in-house counsel members, commented “[a]fter the decision, we all made frowny faces, but then we got down to work.” Keeping in its tradition of being an advocate for transparency, Google has been open and candid about its process of implementing the new RTBF policy every step of the way. The company assembled a comprehensive team of legal professionals to handle the massive influx of RTBF requests. As of September 21, 2015, Google has received a total of 318,269 RTBF takedown requests and has evaluated 1,126,518 unique website addresses for removal.

---

85 Toobin, supra note 81.
86 Id.
90 See generally Goddard v. Google, 2008 WL 5245490, 2008 U.S. Dist. LEXIS 101890 (N.D. Cal. Dec. 17, 2008) (where the court found Google to be immune from illegal conduct of a third party under § 230(c)(1) of the Communications Decency Act because the search engine did not encourage or contribute to the illegal activity).
91 Peter Barron, Google’s Director of Communications for Europe, commented that “[t]he European court of justice ruling was not something that we wanted, but it is now the law in Europe, and we are obliged to comply with that law. We are aiming to deal with it as responsibly as possible. We have had more than 70,000 requests so far. It’s a very big process, it’s a learning process, we are listening to the feedback and we are working our way through that.” Weaver, supra note 84.
92 Toobin, supra note 81.
94 Toobin, supra note 81.
95 GOOGLE, Transparency Report, supra note 3.
2. **Small Internet Companies Lack Resources to Effectively Police Content**

Google is fortunate in its ability to quickly and efficiently organize an extensive dedicated task force in response to the new RTBF policy. However, not all search engine companies have the same resources. Baroness Usha Prashar, Chair of the House of Lords Home Affairs EU Sub-Committee pointed out that the new RTBF policy “would put an unreasonable burden on small search engines, in terms of dealing with requests to remove information.”96 Larry Page, co-founder of Google, weighed in on the onerous regulatory burden that the new RTBF policy imposes on startup companies in comparison to his own:

> We’re a big company and we can respond to these kind of concerns and spend money on them and deal with them, it’s not a problem for us . . . But as a whole, as we regulate the Internet, I think we’re not going to see the kind of innovation we’ve seen.”97

Non-compliance with the new RTBF policy could result in companies facing “fines of up to 5% of their annual global turnover, or €100 million if greater.”98

In order to manage the onslaught of RTBF requests on a case-by-case basis, each company would need to furnish a considerable compliance team.99

3. **The Three-Step RTBF Process for Takedown Requests is Not Practical for Private Companies to Implement**

European Parliament Member and former EU Commissioner Viviane Reding surmised that Google should not have a problem implementing the new RTBF takedown request policy because it is a “small thing” compared to the millions of copyright takedown requests it fields every month.100 Reding used

96 Peers Say ‘Right to be Forgotten’ Principle Unreasonable, supra note 82.
97 Waters, Google Bows to EU Privacy Ruling, supra note 33.
100 Alex Hern, EU Commissioner: Right to be Forgotten is No Harder to Enforce Than Copyright, GUARDIAN (June 4, 2014, 8:12 AM), http://www.theguardian.com/technology/2014/jun/04/eu-commissioner-right-to-be-forgotten-enforce-copyright-google.
these statistics to conveniently gloss over the fact that copyright ownership is much easier to prove than verifying and determining RTBF privacy rights.\footnote{See generally Carolyn E. Wright, Two Easy Steps for Using the DMCA Takedown Notice to Battle Copyright Infringement, NPPA, https://nppa.org/page/5617 (last visited Jan. 25, 2015). “Takedown requests are easily made through a web form, and take an average of six hours for Google to process.” Ben Richmond, Copyright Takedown Requests to Google Have Doubled Since Last Year, MOTHERBOARD (Dec. 2, 2013, 1:05 PM), http://motherboard.vice.com/blog/copyright-takedown-requests-to-google-have-doubled-since-last-year.}

The process involved for a data controller to handle an RTBF takedown request requires a complex three-step process, versus the comparably simplistic one-step process required to handle a copyright takedown request.\footnote{Compare David Drummond, We Need to Talk About the Right to be Forgotten, GUARDIAN (July 10, 2014, 5:05 PM), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate (explaining the complex process and difficulties involved with processing each RTBF request, highlighting that there is no streamlined or easy way to go about the task), with Creative Commons DMCA Notice & Takedown Procedure, CREATIVE COMMONS, http://creativecommons.org/dmca (last visited Feb. 12, 2015) (showing one example of the relatively simplistic process of making DMCA takedown requests).}

First, the data controller must verify the identity and citizenship status of the person asserting the request.\footnote{Dave Lee, Google Sets Up ‘Right to be Forgotten’ Form After EU Ruling, BBC NEWS (May 30, 2014, 7:36 AM), http://www.bbc.com/news/technology-27631001.} Google has revealed that it is a common occurrence for the company to receive “fraudulent removal requests from people impersonating others, trying to harm competitors, or improperly seeking to suppress legal information.”\footnote{Id.} The data controller’s ability to verify a requestor’s identity is limited by its lack of direct access to governmental records to compare the validity of documentation provided. Second, the data controller must determine whether the information at the heart of the request is adequate to be considered for removal.\footnote{Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González, 2014 EUR-Lex 62012CJ013, ¶ 14 (May 13, 2014), http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN.} To do so, the data controller must investigate the claims underlying the RTBF request to determine if the information is “inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes of the processing.”\footnote{Id. ¶ 100 n.4.} Third, the privacy interest of the requestor must be balanced against the public’s interest in the availability of the information.\footnote{Id.} Verifying copyright ownership, in comparison, does not require any comparable balancing test that demands subjective discretion by the data controller. The only step a data controller must take in deciding whether or not to honor a copyright takedown request is to verify ownership of
the copyright in question. The task of verifying copyright ownership is significantly less daunting because most countries provide searchable online copyright databases.108

Comparing RTBF privacy rights to the protection of copyrights is an error of false equivalence. Copyright law, unlike the RTBF policy, is deeply rooted in European statutory law, dating as far back as the 1710 Statute of Anne.109 Its evolution alongside society is evident in subsequent statutes and international treaties implemented over the past three centuries.110 Google’s compliance to copyright takedown requests is directly linked to several well-established international agreements put forth by the World Intellectual Property Organization (WIPO), dating back to the 1886 Berne Convention.111 The agreements clearly spell out in detail the rights afforded to copyright owners to control the use and dissemination of their works.112 These copyrights are absolute and only a few limited exceptions are carved out, such as fair use and fair dealings.113

In comparison, RTBF privacy rights are a relatively new concept and have not been as clearly enumerated. Nor is it easily determinable as to whether a particular RTBF claim is strong enough to warrant absolute control of the information by the individual asserting it. The EU has explicitly said that RTBF privacy rights are not absolute and therefore must be balanced against public interest and other fundamental rights, such as speech, on a case by case basis.114 It is grossly misleading to compare the task of verifying copyright ownership registration, which is regulated by international treaties and maintained by each country within designated governmental offices, with the task of balancing an individual’s personal rights against the greater public’s interest in access to information to determine whether an RTBF takedown request is justifiable.

109 8 Ann. c. 19 (1710) (UK).
111 See generally Berne Convention, supra note 110.
113 Berne Convention, supra note 110, art. 10.
114 See Factsheet on the "Right to be Forgotten" Ruling, supra note 2.
By making this false equivalence argument, the EU is not only over simplifying the responsibility it is imposing on the search engine industry, it is also attempting to dodge the bigger bullet of the Costeja ruling: the empowerment of private entities such as Google with the authority to act as judge and jury in the implementation of personal privacy rights on the Internet.\footnote{Julia Powles, Google’s Grand European Tour Aims to Map Out the Future of Data Ethics, GUARDIAN (Sept. 10, 2014, 8:25 AM), http://www.theguardian.com/technology/2014/sep/10/google-europe-explain-right-forgotten-eric-schmidt-article-29.}

C. Undue Burden on EU Member States: Strain on Local Jurisdictions and Inconsistent Results Abound

Policy implementation among several autonomous nations often results in stumbling blocks,\footnote{See CHRISTOPHER HILL & MICHAEL SMITH, INTERNATIONAL RELATIONS AND THE EUROPEAN UNION 172 (2d ed. 2011).} and the attempt to coordinate the RTBF policy among the twenty-eight Member States of the EU is no exception. Member States are dealing with the clogging of their appeals courts and overburdening of their local Data Protection Agencies when search engines refuse to honor RTBF takedown requests,\footnote{WP29 Guidelines, supra note 7, at 12.} the guideline suggestions from the Data Protection Working Party mandate universal implementation of the RTBF on the internet;\footnote{Id. at 3.} there is disagreement between Member States over the core principles and implementation of the new RTBF policy;\footnote{Compare Mark Scott, French Official Campaigns to Make ‘Right to be Forgotten’ Global, N.Y. TIMES (Dec. 3, 2014, 4:19 PM) [hereinafter Scott, French Official Campaigns], http://bits.blogs.nytimes.com/2014/12/03/french-official-campaigns-to-make-right-to-be-forgotten-global/?_r=0 (reporting that French officials support the new RTBF implementation policy), with Patrick Donahue & Cornelius Rahn, Germany Nulls Arbitration for Web ‘Right to be Forgotten’, BLOOMBERG NEWS (May 27, 2014), http://www.bloomberg.com/news/articles/2014-05-27/germany-nulls-arbitration-for-web-right-to-be-forgotten (reporting that German officials approach the new RTBF policy with caution), and UK SUB-COMMITTEE REPORT, supra note 8 (reporting that British officials oppose and reject many aspects of the new RTBF policy).} and there are overall concerns of inconsistent decisions across different jurisdictions.\footnote{Data Protection Reform: Frequently Asked Questions, EUROPEAN COMMISSION (Jan. 25, 2012), http://europa.eu/rapid/press-release_MEMO-12-41_en.htm?locale=en [hereinafter Data Protection Reform: FAQ].}

On November 26, 2014, the WP29 released guidelines for the implementation of the Costeja judgment.\footnote{WP29 Guidelines, supra note 7, at 7.} In these guidelines, the WP29 reinforced that search engines, as data controllers, would be required to handle
takedown requests from citizens directly. If a search engine rejects a citizen’s request, either in part or in whole, the citizen may then appeal to either their local official Data Protection Agency (DPA), or alternatively to their local judicial system to verify whether the rejection is proper. Currently, each EU Member State has a single local DPA, and these local DPAs are operated independently from one another. Within only four months after the initial Costeja judgment, at least ninety such appeals were filed with local DPAs in various Member States. At the six-month mark, 440 individual complaints involving Google’s implementation of the new policy had been received by regulators in the United Kingdom, Germany and France. The United Kingdom expressed concern in a report released by the House of Lords that this method of handling the takedown requests would put excessive strain on the country’s local DPA.

The WP29 also instructed search engines to apply RTBF takedown requests across all “all relevant domains, including .com.” This would mean, for example, that if a French citizen makes a controversial RTBF takedown request that the French judicial system ultimately honors, Google would be required to remove the search results from not only Google.fr, but also Google.com (United States), Google.co.uk (United Kingdom), Google.de (Germany), and all other Google domains. Therefore, if search engines and other data controllers comply with this principle, the effects of an RTBF decision in one country’s court system would have global enforcement throughout the Internet worldwide.

Google’s Executive Chairman, Eric Schmidt, opined that the scope of the new RTBF policy applies exclusively to the jurisdiction of the Member States of the EU, and therefore removals should only affect Internet domain addresses that directly correspond to those territories, and not extend to domains that are default pages for other jurisdictions, such as Google.com, which is the default

---

122 Id.
123 Id. at 12.
127 UK SUB-COMMITTEE REPORT, supra note 8, ¶ 38.
128 WP29 Guidelines, supra note 7, at 3.
territory domain only for the United States. Schmidt says this approach is justified because “[a] very small percentage—less than 5 per cent—of European traffic goes to .com so 95 per cent or more are to these sites.” Peter Fleischer, Google’s Global Privacy Counsel, also emphasized that applying the RTBF decision universally would be problematic because “[o]ther courts in other parts of the world would never have reached the result that the European Court of Justice reached.”

Member States do not even agree on how to implement the new RTBF policy, or whether it should be scrapped altogether and re-built from scratch. Isabelle Falque-Pierrotin, head of France’s DPA and Chairman of the WP29, staunchly supports implementation of the new policy in addition to expanding the ruling to include universal jurisdiction over all search engines. Falque-Pierrotin believes that “[t]he location of the search user, not the search engine, is the most important [factor].” In comparison, German officials have been more critical of the new policy and careful of its immediate implementation. Within weeks of the initial Costeja ruling, the Interior Ministry of Berlin released an official statement that it was considering whether to establish special RTBF arbitration courts to aid in the process of deciding what information is suitable for removal from Internet search results. The Ministry reasoned that unchecked power to hide information would be subject to abuse by “[p]oliticians, prominent figures and other persons who are reported about in public.” This caveat could effectively provide these public figures with the means to “hide or even delete reports they find unpleasant,” further lamenting “that the removal of information shouldn’t be left to company algorithms.”

130 Id.
131 Schechner & Robinson, supra note 126.
132 Compare Scott, French Official Campaigns, supra note 119, with Donahue & Rahn, supra note 119 (reporting that German officials approach the new RTBF policy with caution), and UK SUB-COMMITTEE REPORT, supra note 8 (reporting that British officials oppose and reject many aspects of the new RTBF policy).
133 Scott, French Official Campaigns, supra note 119.
134 Id.
135 Donahue & Rahn, supra note 119, Matt Brian, What You Need to Know About the ‘Right to be Forgotten’ On Google, ENGADGET (June 2, 2014), http://www.engadget.com/2014/06/02/right-to-be-forgotten-explainer/.
136 Id.
137 Donahue & Rahn, supra note 119.
138 Donahue & Rahn, supra note 119; Brian, supra note 135.
Of all of the EU’s twenty-eight Member States, the United Kingdom has taken the most hostile stance against the new RTBF policy.\textsuperscript{139} The House of Lords expressed that they do “not trust Google’s judgment” and are “deeply uncomfortable” with the idea of “leaving such judgments to commercial enterprises.”\textsuperscript{140} The Sub-Committee concluded that:

\begin{quote}
[T]he Government does not support the right to be forgotten as it is currently proposed by the European Commission . . . 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 information, and transmission of it—and the impracticality of the practice.\textsuperscript{141}
\end{quote}

In addition to disagreeing about the features and implementation of the new RTBF policy, Member States previously were unable to uniformly implement the 1995 Data Protection Directive that is at the core of the RTBF policy.\textsuperscript{142} A memo from the European Commission in 2012 reported that “differences in the way that each Member State implements the law have led to inconsistencies, which create complexity, legal uncertainty and administrative costs.”\textsuperscript{143} The European Commission proposed a “consistency mechanism” to help solve this problem.\textsuperscript{144} Essentially, the consistency mechanism would be a centralized DPA to handle issues affecting multiple European jurisdictions, instead of asking local DPAs to make those decisions, which reflects the current RTBF implementation model.\textsuperscript{145} However, two years after the proposal for a Centralized DPA, the European Commission has yet to create such an institution,\textsuperscript{146} and the Commission’s post-\textit{Costeja} guidelines clearly instruct for universal application of privacy decisions to be determined first by private data controllers, and then by local DPAs or judicial systems.\textsuperscript{147} This approach to
inconsistency in itself is paradoxically inconsistent, with the European Commission appearing to put the proverbial cart before the horse. The motive for this approach is unclear, and with the continuing accumulation of issues surrounding the new RTBF policy implementation, the strategy appears to be equally unwise.

III. PROPOSAL—A CENTRALIZED DPA AS IMPLEMENTATION SOLUTION FOR THE NEW RTBF POLICY

The WP29’s guidelines for the new RTBF policy do not resolve the major problems that the current implementation of the policy creates for citizens, the Internet industry, and Member States. The solution proposed by the European Commission in 2012 to create a Centralized DPA is altogether ignored by the guidelines released by the WP29. Most confusingly, although the European Parliament has shown recent hostility towards American Internet conglomerates such as Google, the WP29 proposes to entrust these same companies with the power to handle the privacy rights of its citizens and conduct global censorship accordingly.

The current WP29 guidelines are not adequate to address the problems created by the new RTBF policy. However, a Centralized DPA as previously proposed by the European Commission could still be established, and would significantly aid citizens, the Internet industry, and Member States by implementing the new RTBF policy in a coherent and manageable fashion.

A. How Citizens Could Benefit from a Centralized DPA

As the EU holds the RTBF as an important and fundamental right that applies to all citizens, it stands to reason that the EU should take steps necessary to ensure that all citizens, not just those with the necessary resources, are provided with reasonable access to this right.

The first problem for citizens is that in order to make an RTBF request, they must do so online. A Centralized DPA could streamline a variety of options for citizens to make requests, such as via postal mail or telephone, in

148 Id.
150 See generally WP29 Guidelines, supra note 7, at 7.
151 See supra Part III.A.
addition to forms on the Internet. A Centralized DPA could potentially have access to certain government records controlled by the EU as a whole. Therefore, a Centralized DPA may be able to verify identification of citizens via the telephone using specific forms of European-wide identification, such as the citizen’s Taxpayer Identification Number\textsuperscript{152} or European Health Insurance Number.\textsuperscript{153} With proper organization, a Centralized DPA should be able to meet the needs of citizens who are either disadvantaged or simply lack the technological ability to chase down data controllers online and submit direct requests to them via the Internet.

The current WP29 guidelines require citizens to submit unique requests directly to each individual data controller, such as Google or Bing, with no guarantee that all of the data controllers will reach a unified decision to honor the request.\textsuperscript{154} If the citizen’s request is denied by any of the data controllers, they must take further steps to appeal their claim to either their local DPA and/or their local court.\textsuperscript{155} The RTBF process would be more efficient if a citizen could submit one request directly to a Centralized DPA, where a trained agent could analyze the information being requested for removal and apply the three-step process of (1) verifying the identity of the requestor, (2) deciding whether the information qualifies as the kind that may be considered for the RTBF policy, and finally (3) balancing the interests of the individual’s right to privacy with the public’s right to knowledge of the information. Only after all of these steps are applied to the citizen’s particular request and deemed to be approved for removal, may the agent contact the data controllers and make a formal order for that information to be removed from the search results and/or servers. This would create uniform removals across all data controllers, and the question as to whether or not a data controller complies with the request under the law would be clear because it would be handling a request made directly by an agency of the EU. This method further removes the burden from the citizen of having to approach each and every data controller to request removal of the same information, eliminating the necessity for that citizen to repeat the same process multiple times over with the risk of varied results. In addition, the Centralized DPA could keep a record of its decisions on file so that if and when new data controllers appear in the future, a citizen would be able to ask


\textsuperscript{154} WP29 Guidelines, supra note 7, at 7.

\textsuperscript{155} Id.
the Centralized DPA to send a copy of the takedown request to the new entities, therefore eliminating the hassle of having to go through the entire request process again.

Alternatively, a Centralized DPA could keep a secure database of all authorized takedown requests, organized in chronological order of decision date, and allow search engine compliance liaisons to access the information with the instruction to check the database regularly (with the option to receive automatic notification digests) and comply with the posted takedown requests accordingly. This method would streamline some of the process by shifting the burden of voluntary compliance onto the data controllers.

Another issue stems from the entrepreneurial community, eager to profit from the challenges facing citizens who want to make RTBF takedown requests.156 Third party companies have already begun to coax citizens into revealing ample amounts of sensitive information by promising to take care of the tedious and difficult requirements of takedown requests.157 This business model exposes citizens to a higher risk of identity theft, with no guarantee that the paid-for request placed by the third party company on their behalf will be successful.158 A Centralized DPA would lower this risk because citizens would be communicating directly with a government agency. Even though government agencies are susceptible to hackers the same as any company connected to the Internet,159 the risk of a citizen encountering a fraudulent third party company merely posing as a legitimate service with the underlying intention of stealing sensitive information would be eliminated. Further, if a Centralized DPA offered RTBF services for free or at the rate of a small processing fee, citizens would not have to deal with handing over money to a private company that does not guarantee results.

B. How the Internet Industry Could Benefit from a Centralized DPA

Google has made it clear that the company does not want to be treated as a data controller, nor does it want the responsibility of deciding difficult

---

156 See Scott, European Companies See Opportunity, supra note 53.
157 Id.
158 Id.
conflicts between privacy rights and public interest. Instead of requiring private Internet companies such as Google to decide RTBF takedown requests, a Centralized DPA could remove this burden by directly accepting and determining the requests. After the Centralized DPA analyzes and makes the ultimate decision as to whether the request should be approved, the DPA could then notify data controllers such as Google of that decision, and provide the companies with a direct order to remove the specific information from search results. This would not contradict the Court’s decision that search engines are data controllers and have a responsibility to honor RTBF requests from citizens, but rather shift the burden of making difficult policy-shaping decisions from the hands of multiple private companies to one public agency.

Both Google and representatives from Member States point out that requiring private Internet companies to process and handle RTBF takedown requests directly creates a considerable burden for small startup companies that lack the abundant resources of giants such as Google or Microsoft to create comprehensive legal teams for handling a large volume of requests adequately. If a Centralized DPA were to solely handle the decision making process of RTBF takedown requests, then that burden would effectively be removed, and the companies would only need to furnish appropriate staff to comply with the approved removals.

The main concern for data controllers and the new RTBF policy is the complicated three-step process involved in determining whether an RTBF request should be honored. Google’s Chief Legal Officer, David Drummond, published an opinion piece where he publicly stated that the company “disagree[s] with the ruling” in part because this process includes “very vague and subjective tests.” Both Google and Member States have voiced disapproval in the discretionary nature of the current policy implementation, allowing private corporate entities such as Google to make

---

160 See Alan Travis & Charles Arthur, EU Court Backs ‘Right to be Forgotten’: Google Must Amend Results on Request, GUARDIAN (May 13, 2014, 9:06 AM), http://www.theguardian.com/technology/2014/may/13/right-to-be-forgotten-eu-court-google-search-results; see also Weaver, supra note 85.

161 Peers Say ‘Right to be Forgotten’ Principle Unreasonable, supra note 82; Waters, Google Bows to EU Privacy Ruling, supra note 33.


163 David Drummond, We Need to Talk About the Right to be Forgotten, GUARDIAN (July 10, 2014, 5:05 PM), http://www.theguardian.com/commentisfree/2014/jul/10/right-to-be-forgotten-european-ruling-google-debate.
impactful decisions on the privacy rights of private citizens and the greater public interest. A Centralized DPA could alleviate this anxiety for both the Internet companies as well as Member States by internalizing the RTBF three-step process, taking that responsibility out of the hands of Google and the like. In addition, a Centralized DPA would be better suited to access personal, sensitive information about citizens in order to verify their identities in a way that Google or any other private company would not and should not have privileged access to.

C. How Local Governments Could Benefit from a Centralized DPA

In 2012, the European Commission admitted that significant problems had arisen from Member States implementing the 1995 Data Protection Directive inconsistently. Their report concluded that this problem “affects the trust and confidence of individuals and the competitiveness of the EU economy.” Despite such a heady internal warning, the WP29, under the supervision of the European Commission, neglected to address this problem in its current RTBF implementation guidelines. Instead, the guidelines instruct citizens to seek remedy in their local jurisdictions if their direct request to the data controller is denied. This method has resulted in complaints from citizens piling up for both local DPAs and appeals courts. As the European Commission originally proposed in 2012, a single data protection authority operating under a streamlined set of rules, such as a Centralized DPA, would combat this issue by creating a “‘one-stop-shop’ for data protection” that would:

[Greatly simplify the way businesses and citizens interact with data protection laws and give incentives to trade and invest cross-border in the internal market, as opposed to the current situation where businesses are supervised by a different authority in each Member State they are established.]

A Centralized DPA would remedy the problem of Member States reaching divergent decisions because the decisions would apply to all territories of the EU. It would be able to recruit representative agents from all twenty-eight

164 Data Protection Reform: FAQ, supra note 120.
165 Id.
166 See generally WP29 Guidelines, supra note 7, at 7.
167 Id. at 8.
169 Data Protection Reform: FAQ, supra note 120.
Member States who could work together to approve takedown requests, creating a more efficient method of removing information across country borders. Controversial topics, such as information regarding politicians, events or other individuals that would potentially have an impact across Member State lines if removed, could be debated in a single forum, rather than allowing a lone Member State to decide whether or not the removal request should be honored.

Although a Centralized DPA would not directly address the issue as to whether RTBF takedown orders should be implemented universally on the Internet to include domain names hosted outside of the EU,\(^{170}\) it would be in a better position than Google or any other outside foreign entity to make takedown decisions that could be honored across all European domains.

Some Member States of the EU have been particularly vocal in their criticism of allowing corporate entities such as Google to shape public policy by having the first crack at approving RTBF takedown requests.\(^{171}\) Germany has pointed out that politicians and other prominent figures could use this to their advantage by manipulating information available to the public.\(^{172}\) A Centralized DPA could solve this by making RTBF takedown decisions before any official order would be passed down to the data controller, effectively eliminating the role of data controller as policy maker.

**CONCLUSION: THE BEST PRACTICE OF “FORGETTING”**

* I’d always maintained that much of the anarchy and craziness of the early internet had a lot to do with the fact that governments just hadn’t realised it was there . . . As we move more and more of what we do into that non-physical realm, it all becomes terribly important to the people who write the cheques.

—William Gibson\(^ {173}\)

The Internet has become exceptionally valuable and important to society since it was introduced to the general public in the mid-1990s.\(^ {174}\) The

\(^{170}\) *Compare WP29 Guidelines, supra note 7 (ordering universal jurisdiction for RTBF takedowns), with Schechner & Robinson, supra note 126, at 3–4 (“Other courts in other parts of the world would never have reached the result that the European Court of Justice reached.”).*

\(^{171}\) *See UK SUB-COMMITTEE REPORT, supra note 8; see also Donahue & Rahn, supra note 119; Brian, supra note 135.*

\(^{172}\) *Brian, supra note 135.*

\(^{173}\) *Steven Poole, Tomorrow’s Man, GUARDIAN (May 3, 2003, 6:40 PM), http://www.theguardian.com/books/2003/may/03/sciencefictionfantasyandhorror.williangibson.*
percentage of the world’s population using the Internet doubled from twenty
percent in 2005 to forty percent in 2014.175 It has become the main source in
developed countries for news, entertainment, and communication. The more
predominant the Internet becomes in society, however, the greater the need is
to regulate it. Forward-thinking governments, such as the EU, understand the
importance of protecting the fundamental rights and freedoms of its people in
this new virtual landscape. The protection of citizens’ fundamental rights to
privacy is the backbone of the RTBF policy as well as the Costeja opinion. The
problem is not with the principle of the policy, but with the way it has been put
into practice.

The European Commission was on track in 2012 with the assessment that a
“one-stop shop” would be the best consistency mechanism for ensuring
uniform enforcement and observance of current and future privacy laws.176 The
exact reason why this method of implementation has yet to be explored post-
Costeja is not clear, with some sources reporting that the search engine
companies themselves have complained about the approach,177 while others
cite certain Member States for the resistance.178 Regardless of who is to blame
for blocking implementation of the idea, this Comment comprehensively
outlines the numerous solutions a Centralized DPA would provide.

A Centralized DPA would not provide a magic bullet for the other
remaining issues that stem from implementation of the RTBF policy. For
example, a Centralized DPA would not solve the argument as to whether
RTBF takedown orders should be honored universally on the Internet to
include domain names hosted outside of the EU.179 However, it could
determine that the RTBF decisions be honored for all domain names hosted
within the EU, and therefore a decision regarding any EU citizen should be
binding on domain names hosted in all Member States.

174 Brief History of the Internet, INTERNET SOC’Y, http://www.internetsociety.org/internet/what-
176 Data Protection Reform: FAQ, supra note 120.
177 Jean De Ruyt & Sebastian F.A. Vos, The EU Data Protection Regulation After 3 Years of Negotiation,
NAT’L L. R. (Jan. 6, 2015), http://www.natlawreview.com/article/eu-data-protection-regulation-after-3-years-
negotiation.
178 Jeremy Fleming, EU Lawmaker Warns of Data Protection Rules Delay Till 2016, EURACTIV (Jan. 8,
2015, 7:42 AM), http://www.euractiv.com/sections/infosociety/eu-lawmaker-warns-data-protection-rules-
delay-till-2016-311100.
179 See supra Part IV.C.
It would not be feasible to enforce RTBF takedown orders universally because of a significant difference in global ideologies on protected speech. The United States is a prime example of a country that notoriously holds the constitutional right to freedom of speech as paramount to individual privacy rights. It is unlikely that the United States would allow censorship of any search engine’s results, particularly because the courts have held that search results are fully protected by the First Amendment of the Constitution.

A significant caveat in attempting to make laws around technology is that technology is always changing, and therefore it is difficult to create regulations fast enough to keep up with its constant evolution. The EU is making a valiant effort to protect its citizens in light of the way the Internet has impacted society, and a Centralized DPA appears to be the most sensible step forward in ensuring citizen’s rights to privacy on the Internet.

BUNNY SANDEFUR

---


182 “Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect.” Zeran v. America Online, 129 F.3d 327, 331 (4th Cir. 1997); EUGENE VOLOKH & DONALD M. FALK, FIRST AMENDMENT PROTECTION FOR SEARCH ENGINE SEARCH RESULTS 6 (Apr. 20, 2012), http://www.volokh.com/wp-content/uploads/2012/05/SearchEngineFirstAmendment.pdf.

183 Moore’s Law explains how the limits of electronic technology is exponentially endless, with the average rate of processing growth predicted to double every two years. See generally Gordon E. Moore, Cramming More Components Onto Integrated Circuits, 86 PROC. IEEE 82, 84 (1998).

*Executive Managing Editor, Emory International Law Review; J.D. Candidate, Emory University School of Law (2016); B.A., International Studies, summa cum laude, University of Miami (2011). Thank you to Dr. Liza Vertinsky for all of her brilliant guidance and encouragement; thanks to my editor, Sarah Kelsey, for being a beacon of perfection; special thanks to my parents, Mary & Michael Weiskott, as well as Dr. Ryan Lake, for the superabundance of love and support.