media LAWS
Law and Policy of the Media in a Comparative Perspective

Law and Media Working Paper Series

no. 16/2016

STEFANO AMPRIMO*

The Right to be Forgotten, determining the liability of ISP as media platforms and paving the way to a regulated future

SUMMARY: 1. A Right to be Forgotten. - 2. The implications of an Internet-connected society. - 3. ISPs as media platforms. - 4. Drawing a line between 'significant' and 'forgettable' content. The 'Right to Know' what? – 5. A future for the Right to be Forgotten.

* LLB Candidate at Universidad de Lima, Legal Intern at Amprimo & Flury Abogado

Law and Media Working Paper Series

Codice ISSN: 2531-484X

EDITORE: Oreste Pollicino - COORDINATORE EDITORIALE: Marco Bassini

SEDE: Via Roentgen, 1 – 20136 Milano e-mail: submissions@medialaws.eu

"People always talk about how hard it can be to remember things - where they left their keys, or the name of an acquaintance - but no one ever talks about how much effort we put into forgetting. I am exhausted from the effort to forget... There are things that have to be forgotten if you want to go on living."

Stephen Carpenter, Killer

1. *A Right to be Forgotten.*

"There are things that have to be forgotten if you want to go on living"[1].

The premise revolving around the so-called Right to be Forgotten or Right to Oblivion that has Internet Service Providers (hereafter, 'ISPs') weighing the importance of conflicting rights such as the Right to Digital Privacy and the rights of freedom of speech and access to information (hereafter, 'right to know') revolves around the idea that data subjects have a right to control the publicity of content available online that could be considered misleading, inaccurate, false or otherwise outdated and therefore a threat to other constitutionally-protected rights. As such, the question as to just how much control should data subjects have over the processed data and how such control may affect third parties' rights arises as one of the core considerations in the right to be forgotten debate. At a glance one might think that the answer is fairly obvious: as an individual right, privacy should be left in the hands of individuals, letting them decide how far they divest themselves from their own right to privacy. Nonetheless, the individualist answer is not the only answer. A collectivist point of view must be considered, paying especial attention to the implications of an 'absolute' right to be forgotten on censorship, the right to conduct business (alluding to the specific case of news publishers) and the collective right to know. The matter is incredibly relative, for, as Franco

[1] S. CARPENTER, *Killer*, n.p., Stephen Carpenter, 2010.

Pizzetti puts it *"There is no doubt, in fact, that humans always live an "existential" contradiction. On the one hand, they aspire to immortality, and, knowing that they cannot have it, they try to leave the memory of themselves for as long as possible as the only way to prolong their life, or rather their memory into the future that they existed, and what they achieved. (…) Conversely, every person also has the terror that every negative act committed in the course of their existence can be remembered forever or at least while he is alive and so are the ones who have memory."*[2] With this in mind, it becomes incredibly difficult to come up with an absolute answer to whether or not a right to be forgotten should be legally and universally recognised.

Indeed, several parties worldwide, including judiciary authorities, competent administrative authorities and scholars have weighed in the debate through decisions and opinions supporting both sides of the matter. To illustrate, on February 2012 Jeffrey Rosen published an article on the Stanford Law Review comparing the approaches that the US and EU were adopting towards what was then a still young and abstract right to be forgotten, venting several concerns, particularly concerning the broadness of the EU's definition of the right to be forgotten[3]. Likewise, Farhaan Uddin Ahmed, a law scholar, while supportive of the recognition of a right to be forgotten, has some serious reservations regarding the current applicability and implementation of the system, remaining especially concerned about the power being conferred to ISPs, given the conflicts of interest that may arise given their business-oriented policies[4]. Conversely, in March, the *Commission Nationale de L'informatique et des Libertés* (CNIL) confirmed the existence of a global right to be forgotten by issuing a 100,000 euros fine against Google for failing to remove right to be forgotten requests from global search results, limiting the removal to the '.fr.' domain only; Google has, since, appealed

[2] F. PIZZETTI, *Privacy E Il Diritto Europeo Alla Protezione Dei Dati Personali: Dalla Direttiva 95/46 Al Nuovo Regolamento Europeo,* Torino, Vol. 4, p. 20, G. Giappichelli Editore, 2016.
[3] J. ROSEN, *"The Right to Be Forgotten", Stanford Law Review,* Issue 88, Volume 64, Feb. 2012.
[4] F. AHMED, *"Right to Be Forgotten: A Critique of the Post-Costeja González Paradigm" Academia.edu. Computer and Telecommunications Law Review*, Westlaw UK, Aug. 2015.

this decision to France's highest administrative court, the Conseil d'État, which can take the case or refer it back to the EU high court[5].

Nonetheless, the most significant impact on the debate came on May 2014 with the European Court of Justice's (hereafter, 'ECJ') landmark decision on the *Google Spain & Google Inc. v. Agencia Española de Protección de Datos (AEPD) & Mario Costeja González* (hereafter, 'Google Spain' or 'Case C-131/12') case, where the ECJ clearly defined the rights to data protection and privacy as the rights at stake, as well as their legal protection and extent through the interpretation of Articles 7 and 8 of the European Charter of Fundamental Rights (hereafter, the 'Charter') and current Data Protection legislation, alluding to the concepts of adequacy, relevance and proportionality to evaluate the prevalence of the opposing rights. Consequentially, this decision produced a paradigm shift, which resulted in two essential pieces of jurisprudence: Firstly, it established that users that felt that any of their fundamental rights was being hurt by search engine's results had a 'right be forgotten'; secondly, it established that Google and other search engines were 'Data Controllers', as opposed to mere 'Data Processors' under Directive 95/46/EC (hereafter the 'Data Protection Directive' or 'DPD'). These provisions had serious repercussions in the way takedown requests were handled by European authorities and ISPs.

Most recently, on 29 April 2016 –nearly two years after Google Spain– the Belgian Court of Cassation decided on the *Olivier G v. Le Soir* case, ruling favourably over the plaintiff's right to be forgotten, applying the principles laid down by the Google Spain ruling to confirm the Court of Appeal's decision to order the anonymisation of a 1994 article published by *Le Soir*, which contained the plaintiff's full name in a story concerning a fatal traffic accident. In this sense, the Court of Cassation argued that *"[Olivier G] fulfills the conditions to benefit from a right to be forgotten, as maintaining a non-anonymised online article many years after the events it describes, is likely to cause him [the plaintiff, defendant in Cassation] disproportionate damage compared to the*

[5] R. LEVINE,*"The 'Right to Be Forgotten' and Other Cyberlaw Cases Go to Court"* Bloomberg, 23 June 2016. Web. 14 Nov. 2016, www.bloomberg.com.

benefits that may arise from the strict respect for the freedom of expression of [the defendant, applicant in Cassation, in application of the conditions of legality, legitimacy and proportionality imposed by Article 10, § 2 of the European Convention on Human Rights and Freedoms"[6], therefore, finding *Le Soir* at fault, given the inadequacy (outdated and no longer newsworthy) and disproportionality of the data processed to achieve its journalistic goals.

Having considered some relevant case law, it is worth mentioning that the existing legislation (Directive 2000/31/EC) already contemplates the removal of malicious content through a notice-and-takedown mechanism, however, no objective guidelines regarding the evaluation of the content's quality exist at this level, essentially leaving it in the hands of national regulators to determine such conditions through national legislation, a non-existing reality, as of yet. It is also worth mentioning that Article 1(5)(b) of Directive 2000/31/EC (hereafter, the 'E-Commerce Directive' or 'ECD') and consideration number 14 of its preamble expressly state that its provisions shall not apply to matters *"questions relating to information society services covered by Directives 95/46/EC and 97/66/EC"*. Indeed, while the DPD protects personal rights, in this case, the rights to privacy and data protection, the ECD protects economic rights such as intellectual property, and deals with the liability of ISPs attending to several situations. Consequently, as cases grow in complexity, it is in the hands of judges to integrate both pieces of legislation in order to (i) determine the prevalence of the opposing rights in right to be forgotten cases applying the DPD's provisions; and, (ii) determine the grade of responsibility of the involved party (ISP), should there be any damages, applying the ECD's provisions.

In this sense, we must ask ourselves to what extent should the right 'of the many' to know prevail over the right 'of the few' to be forgotten and vice versa? The current situation has ISPs determining whether reported content should stay online or be removed based on their own subjective evaluation of the content. That is to say, private companies are exercising a power of constitutional control to decide whether to recognise an individual's right to be forgotten

[6] *Olivier G v. Le Soir*, N° C.15.0052.F Belgian Court of Cassation, April 2016, p. 37. Translated.

or to protect the community's right to know (and right to conduct business), without any prior delegation by a competent public entity. However, should private companies really be playing the role of public regulators in deciding the prevalence of Constitutional rights? Several concerns arise when considering the private interests that may drive an ISP's decision to pull down or keep any given content, especially considering the amplified effect that time has in the world of bits and its contribution to the advent of irreparability of the damage caused by the content. In this regard, these concerns must be carefully analysed in order to come up with a solution that does not sacrifice the integrity of Constitutional liberties to profit-driven decisions, remaining swift and efficient as a tool to minimise the damage caused by malicious content circulating in the world of bits. In order to do so, we must consider how an Internet-connected society has moulded the concepts of information and control.

2. *The Implications of an Internet-connected Society*

Society, social circles, communication and information are concepts no longer tied to geographical boundaries and borders. In this sense, a Norwegian physicist residing in New York can get access to the same lecture given by professor Stephen Hawking at MIT as a Chinese student attending the Georgia Institute of Technology or as an MIT student who physically attended the lecture. The development of the Internet and the advancements in broadband speed and accessibility have essentially blurred the line between the physical and digital worlds in such a way that everyone has an equality of opportunities and stands and equal chance to access the knowledge scattered across the globe.

The reality is that the rise of the Internet as a communication standard –and, essentially, a right– has unequivocally democratised the notion of access to information, enabling anyone to access a near-infinite source of information, being able to read it, replicate it and use it to create more content. Therefore, an identical copy of the same line of code can be found in two

or more different places and under the control of two or more different agents, simultaneously, at any given moment. This begs the questions, who 'owns' the Internet? Who 'holds' the information available in the Internet? And, who 'decides' how the information is used, when it should be made available and when it should be taken down? The answer to these inquiries is simple, although its explanation is far more complex. No individual person, organisation or entity has control over the Internet and its internal operability, as the ease with which a user can upload, say, a video, and other users can make millions of copies of that online file, store them in their hard drives and upload them to different platforms has made monitoring, regulating and controlling data traffic a near-impossible task with the currently available technological tools. As such, nobody can singlehandedly guarantee the destruction of a certain content from the Internet without having to wipe the entirety of servers that compose it, as time plays an essential role in the propagation of data, thus diminishing the control that the original agent has over the published content with every elapsed second. Indeed, as the Tesla and SpaceX CEO, Elon Musk put it –referring to an essay he published in the Huffington Post and then requested to be taken down– *"You can always find things on the Internet. So, it's not like it's [the content] gone. It's just not easily found"*[7].

As previously noted, in the European scene, the E-Commerce Directive has made an attempt to regulate the removal of content as per the request of users, introducing a notice-and-takedown procedure that is to be triggered by any interested party. However, the system has several caveats, such as the fact that the legal validity of a takedown request can be subjected to additional requirements as per individual national implementation law, such as the case of Article 16(b) of the Italian Legislative Decree 70/2003, which states that Hosting Providers remain exempt of any liability, so long as *"as soon as it becomes aware of those facts, through the communication of the competent authorities, acts expeditiously to remove or to disable*

[7] A. VANCE, *Elon Musk: Tesla, SpaceX, and the Quest for a Fantastic Future,* New York, NY: Ecco, HarperCollinsPublishers, 2015.

access to the information"[8] (emphasised by the author). Indeed, while Article 14(b) § 4 of the ECD requires ISPs to remove the infringing content after *"obtaining such knowledge or awareness"*[9] from any source, the Italian implementation decree introduces the requirement of "official notice by a competent authority" and, while this requirement does not preclude the user from submitting the takedown request directly, it effectively allows ISPs profiting from the data to hold off the takedown until the official notice is delivered, essentially subjecting the removal process to the bureaucracy of the public administration or the good graces of the ISP to put aside its own interests and remove the content in the spirit set by the E-Commerce Directive, however this is highly unlikely, as seen in cases such as *Google v. ViviDown*, where the content was not taken down until an injunction was granted, and most recently, the untimely removal of the content that lead to Tiziana Cantone's decision to commit suicide. All things considered, it is important to remember that, while the decision over the removal of content does not lie solely on the ISP and users can also turn to the competent authority, the latter constitutes a much slower mechanism that can often result in late, ineffective measures.

With this in mind, the role of the data controller –as defined by the Data Protection Directive– becomes very important in the protection of the data subject's rights, as failing to take down the infringing content in a diligent and timely manner can result in the damage turning irreparable. However, the development of this idea then turns to the question: Who is the data controller? Can traditional Hosting Providers be considered data controllers and thus be subjected to Section 4 of the ECD? Or does this liability remain exclusive to the original uploader that processed the data subject's personal data? *Google v. Vivi Down* provided some valuable insight into this matter, providing the notion of multiple relationships that can

[8] Article 14, letter b) of Decreto Legislativo del 9 aprile 2003, n.70, "Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno", Italy. Translated.

[9] Article 14, letter (b), §4 of Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

determine the role of each of the parties at stake in relation to one another. In the case at hand, Google and some of its top executives were sued by ViviDown, an organisation dedicated to the aid of children diagnosed with Down's syndrome, on the charges of defamation and illegal data processing for hosting a video depicting a few schoolboys bullying one of their classmates who suffered of autism, mistakenly alluding at Down's syndrome and bringing up ViviDown in their harassment. The first instance decision acquitted Google from the defamation claims, explaining that it had no knowledge of the contents of the video in order to be able to confirm the veracity of the information; Article 15 of the E-Commerce Directive was used to explain that Google was in no obligation to monitor the content of what its users uploaded. On the other hand, Google and its executives were convicted of the crime of illegal data processing, on the grounds of having failed to obtain a valid form of consent from the data subject (the bullied boy) before processing his day. The decision was quite contradictory, as requiring that the ISP request the consent of the data subject inherently requires it to have knowledge of the content beforehand, violating Article 15, which was used as the justification for the former acquittal.

Quite unsurprisingly, Google appealed the decision and the Court of Appeals acquitted Google from both indictments, alluding at the obvious contradictions in the previous decision. This decision was later confirmed by the Supreme Court. The argument that made a difference in both the Court of Appeals and the Supreme Court was Google's theory regarding the relationships that existed between the different parties in the case. Google, Inc.'s defence attorneys explained that three different relationships existed:

(i) the relationship between Google and the user of Google Video (namely, the uploader), where Google was the data controller only regarding the personal data of the uploader;

(ii) the relationship between the uploader and the bullied boy (the data subject), where the data controller was the uploader, as it was her who had control over the content and how it was being purposed; and,

(iii) the relationship between Google and the affected data subject, which they referred to as a "non-relationship", alluding to the fact that *"Google was not aware of the video, of the boy and of his personal data, therefore it did not make any decision regarding the data processing, which occurred under the control of the uploader"*[10]. As such, Google would remain exempt of any liability given its lack of knowledge or control over the content or the data subject's personal data.

Indeed, Google's rhetoric provides a practical way to define the roles of each party by disseminating the different activities being carried out and the party over which said activities have effects on. Therefore, whereas in the past search engines such as Google would be considered mere Hosting Providers and thus 'mere conduits' exempt from any form of liability, as provided by Article 14(b) § 4 of the E-Commerce Directive

Nonetheless, this changes once an ISP becomes more than a mere hosting provider and begins performing further operations, such as exercising editorial power over its data transit.

3. *ISPs as Media Platforms.*

In the previous section, we explained the implications of an Internet-connected society and its ramifications in the liability of ISPs, alluding to exemption enjoyed by this type of services. Yet, the question of whether online platforms such as Google and Facebook are in fact media platforms in disguise becomes particularly relevant in those cases where the action to remove the unwanted content has come too late and liability and damages become the central scope

[10] E. APA and O. POLLICINO, *Modeling the Liability of Internet Service Providers, Google vs. Vivi Down: A Constitutional Perspective*, Egea, Milano, 1st ed, 2013, p. 43.

of case. In cases such as the ones described, ISPs generally insist on the stance that they are hosting providers and that, as such, under Articles 14 and 47 of the E-Commerce Directive they would be exempt from any duty to perform *ex-ante* monitoring over the content uploaded and shared by their users, thus remaining exempt from any liability given their lack of 'actual knowledge' of the content. This would be generally true, except recent case law and a mutation in the behaviour of ISPs and their business models have resulted in a few things: (i) the birth of the distinction between Passive and Active Hosting Providers[11], both of which fall under different degrees of exemption; (ii) the relationship theory; and, most importantly for the matter at hand, (iii) the consideration that some hosting providers may fall under the classification of "media editors". For example, a recent announcement by Joel Kaplan, Facebook's VP of Global Public Policy –a social network whose founder, Mark Zuckerberg, has historically insisted is *"a tech company, not a media company"*[12]– claimed that Facebook will *"begin allowing more items that people find newsworthy, significant, or important to the public interest — even if they might otherwise violate our [Facebook's] standards"*[13]. The mere fact that Facebook is, without any prior notice or user-triggered mechanisms, taking upon itself the task of reviewing which content it deems "newsworthy" or "important to the public interest" means it is performing an imminently editorial operation, effectively putting it between the crosshairs of the EU E-Commerce Directive's liability regime.

Indeed, exercising editorial choice over the data traffic and performing *ex officio* censoring of content by means different to the user-triggered notice-and-takedown mechanism contemplated in the ECD puts Facebook (and other similar services) in an awkward position,

[11] For more information, see *Google v. Vividown case,* n. 5107/14, 17 December 2013, the Italian *Corte di Cassazione*.
[12] *"Facebook CEO: 'We're a Technology Company. We're Not a Media Company"*, CNNMoney, Cable News Network, 07 Nov. 2016. Available at http://money.cnn.com/video/technology/2016/08/29/facebook-ceo-were-a-technology-company-were-not-a-media-company-.cnnmoney/.
[13] *"Input from Community and Partners on Our Community Standards - Facebook Newsroom"*, Facebook Newsroom, 21 Oct. 2016. Available at http://newsroom.fb.com/news/2016/10/input-from-community-and-partners-on-our-community-standards/.

where it cannot enjoy the exemptions granted by Article 14 as it is admittedly performing a form of *ex ante* monitoring that grants it knowledge and awareness of the content of the data uploaded and shared by the platform's users. Nevertheless, in order to establish whether or not Facebook and other ISPs are behaving as editors we must distinguish between the use of data parsing algorithms and human curation. While the former are commonplace in modern technology platforms and are used by services such as Google, Facebook, Twitter to detect and block inherently inappropriate or illegal content that violates the company's terms of service, such as copyrighted material, for example; the latter are a lot more uncommon, depending on human conscience, rather than a computer algorithm. This type of 'curation' is typically used in more complex scenarios, where the correspondence of the data would be hard or not entirely determinable by a machine; a good example of this kind of system can be found in music streaming services such as Apple Music and Tidal, which, among other features, offer their users the creation of human-curated content 'tailored' to their needs, a promise that is hard to achieve using machines when it comes to something as complex as music and the user's taste in it. Therefore, while data parsing algorithms often depend on keywords and other tools, such as acoustic fingerprinting, to filter data without necessarily leading to gaining actual knowledge of the content, human curation inherently entails the ISPs actual knowledge of the content, for otherwise it would be unable to categorise it.

This being said, we must point at the fact that what Facebook's VP of Global Public Policy is referring to in the statement previously cited is human curation, which escapes the scope of its data parsing algorithm, as said algorithm has no way of evaluating when any given content that its system has already categorised as inappropriate should be deemed as "newsworthy" or "important to the public interest"; that is where human curation kicks in and Facebook's 'editors' decide which content stays and which content goes. In this situation, the ISP is actively engaging in an activity through which it is exerting its influence over what the users can see. Consequently, failing to remove infringing content in an expeditious manner –this time without necessarily requiring formal notice– would produce direct liability implications

on the ISP itself, as well as the original data controller. This begs the question, when is it justified for and ISP to keep content that might be considered graphic, sensitive or otherwise hurting of an individual's personal liberties and right to digital privacy? Where do we draw a line between 'newsworthy', relevant information and 'morbid' entertainment and useless, 'forgettable' information?

4. *Drawing a line between 'significant' and 'forgettable' content. The 'right to know' what?*

In times where hate speech, leaks, revenge porn, suicide videos and other graphic contents have become commonplace in the Internet, we must draw the line between content that might in some way be considered 'newsworthy' or relevant to the public interest, and infringing content. For the purposes of this paper, we will allude to the concept of 'morbid entertainment', which we will define as "content characterised by abnormal, unhealthy and unpleasant subjects that possess no social value". As we know, *Handyside v. the UK* set the groundwork for the interpretation of the EU's protection of freedom of speech under Article 10 of the European Convention on Human Rights (hereafter, 'ECHR'). Indeed, paragraph number 49 of the Judgement stated that paragraph 2) of Article 10 ECHR resulted *"applicable not only to 'information' or 'ideas' that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population"*[14], effectively extending the article's protection to cover even what could be considered hateful or shocking 'speech' (content, for the matter at hand). Ultimately, per the Strasbourg Court's judgement, what matters is not the content itself, but rather its relevance and context. To illustrate, Mr. Handyside's work was not censored because of the obscene content it portrayed,

[14] *Handyside v. the United Kingdom*, No. 5493/72, The European Court of Human Rights, Strasbourg, December 1976.

but rather because his work was aimed at and underaged audience, which is why the Court ultimately decided the content had to be censored.

Likewise, the Judgment of the Court (Grand Chamber) of 13 May 2014 (Costeja González Case) had a significant impact in the way processed data is evaluated to determine its relevance and the impact of its removal on the welfare of the rights to access to information (on the internet users' end) and to conduct a business (on the publisher's end). Most significantly, paragraph 72 of the judgement contemplated that *"that they [processed personal data] are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed', that they are 'accurate and, where necessary, kept up to date' (…)"* [15] (emphasis by the author). As such, if the data processing's purpose is to keep the public informed with 'newsworthy' content deemed 'relevant to the public interest', then we must ask ourselves what is 'newsworthy', what is 'relevant to the public interest' and what is the criteria being used by online platforms to evaluate these conditions. In this sense, for the purposes of our analysis, we will be focusing on the adequacy of the data. In this regard, the recent Tiziana Cantone case and the controversy surrounding some of President-elect Donald J. Trump's campaign remarks represent two opposing polar points in this debate.

On the one hand, we have the 45th President of United States, whose campaigning rallies and speeches have sometimes been considered shocking, aggressive and borderline discriminating. However, despite containing a message that may well offend or shock certain viewers, his campaign videos are amongst the most watched and shared videos in social media platforms and have not been subject to any sort of censorship, resulting from the fact that in the context of a presidential election, this 'offensive' content resulted relevant to the public interest, as voters would determine whether to vote or not for President-elect Trump based on the messages poured in said speeches. It is relevant to mention that Mr. Trump's condition of 'public figure' means that privacy protection is a tad more lenient in his case, however, that

[15] *Google v. AEPD & Costeja González*, C-131/12, The Court of Jutice of the European Union, 13 May 2014.

does not change the fact that he, like anyone else, could have suffered some degree of censorship on behalf of content editors. On the other hand, we have the recent Tiziana Cantone case, a victim of revenge porn whose video was kept circulating across social networking platforms until an official injunction ordered Facebook to take down the video. Normally, it would have taken no more than a notification from an interested party (in this case, late Ms. Cantone) in order to get the video taken down, however, shielding behind Italy's flawed implementation of the ECD, Facebook decided to ignore Ms. Cantone's claims to get the video taken down and remained idle until the official notice came knocking at its door. The video was eventually taken down, however, by the time this action was taken, the content had already been watched and replicated millions of times; the damage had turned irreversible resulting from time's amplified effects in the world of bits. Tiziana Cantone committed suicide soon after. Was Tiziana Cantone's video information that could be deemed 'newsworthy', 'relevant to the public interest', perhaps? No, it was simply infringing information, which we classify as 'morbid entertainment', and as such, Facebook should have taken it down as soon as it caught word of its existence. At present, authorities are evaluating whether Facebook should be held liable for Tiziana Cantone's death, and evidence of editorial management of the platform's traffic could easily put lift its hosting provider exemption.

Perhaps the two examples provided in the paragraph above seem too far from each other for us to draw any comparisons, however, consider the following: footage of people jumping off the World Trade Centre (WTC) during the September 11 attacks can be found all over the Internet. Likewise, footage of a young Colombian citizen jumping off the roof of the Sheraton Hotel in Lima, Peru can also be found in the Internet. Now, objectively, these two videos depict the same thing: people jumping off buildings; nevertheless, putting each into context lets us determine their relevance. While the first video, depicting people jumping in an attempt to save their lives during the horrors that took place at the WTC in 2001 could be qualified as newsworthy and ultimately relevant for the community to be aware of the horrors of terrorism, the second video depicts a scene that ultimately has no value to anyone. It depicts

a person taking its own life, accompanied by the morbid commentaries of the people watching and recording, yelling "jump!" or "don't do it"; once again, we are facing what we've called morbid entertainment. Such content has no social relevance and should be considered *per se* infringing and be taken down upon gaining knowledge or receiving notice.

To sum up, we've determined that the social relevance of a given content and its permanence online are largely determined by its context and purpose, hence ruling out the possibility for an objective takedown criterion, instead leading us towards a subjective, case-by-case solution. However, it must be noted that the obvious shift that is taking place in the behaviour of some ISPs will eventually have to be acknowledged both by regulators and the ISPs themselves, and a legislative solution will have to be drawn in order to accommodate the new subclasses of service providers 'hybrids' that are beginning to emerge. Like Facebook, many other social networking or content sharing platforms are taking particular interest in news sharing, a shift that is diversifying the market, making it more dynamic and less biased. However, as previously noted, a legal framework will have to be put in place in order to properly regulate the extent of liability of which these kinds of services will be subjected to.

5. *A future for the right to be forgotten*

Part of the purpose of this article is to come up with possible solutions to the existing caveats in the system that may, in time, make it more reliable, responsive and efficient. Everyone can agree that, while having ISPs handle the evaluation of notice-and-takedown requests is the easiest and most efficient way, it isn't always the most convenient, considering the entrepreneurial motives that might drive their reasoning behind taking down or maintaining a certain alleged infringing content online. Indeed, a public entity imbued with competence should be the one performing such a test, however, State bureaucracy could lead

to an untimely measure, and thus a 'non-solution'. By virtue of these reasons, we consider that a viable control mechanism could be drawn from the following:

1. Pre-emptive blockage of access to the allegedly infringing content upon receiving a set number of complaints (flags) or formal (non-official) notice by an interested party.
2. Send the challenged content over to the national competent authority for evaluation.
3. Competent authority emits a verdict and notifies it through formal conduit. Cases where the competent authority fails to deliver a decision should be turned over to an international body for evaluation.
4. Subsequent deletion or access blockage lift depending on the authority's decision.

By following this algorithm, not only do we ensure a rapid response able to put a stop to the current and potential damage, but it also allows us to evaluate the content and its implications over conflicting rights through a competent, impartial authority imbued with powers to perform concrete (case-by-case) constitutional control. In this sense, while the most efficient option would be to implement an objective set of rules to for the competent authorities to conduct the evaluation of the content, we feel that, given the complexity of the matter, an objective exclusion rule would lend itself to the unfair removal of certain content that might be considered shocking but would still be protected under the wings of Article 10 ECHR and the guidelines set forth in paragraph 72 of the Costeja González Judgement, as concepts such as adequacy and social relevance are hard to evaluate on an objective basis. Instead, the best alternative would involve a subjective evaluation that considers the context, purpose, adequacy and social value of the allegedly infringing content, and is subjected to a set of guidelines aimed at minimising the authority's degree of discretion over the decision.

Indeed, Farhaan Uddin Ahmed supports a similar solution, calling for the creation of "specialised neutral independent bodies" at the national and international levels to decide decide removal request cases on the basis of their individual merits, laying off the burden from ISPs and legitimising the process by "minimising the risk of censorship and exploitation of the

right to be forgotten"[16]. Ahmed goes on to describe three factors that must be accounted for, which correspond with the suggested subjective criteria: (i) time, specifically referred to the 'age' of the published information (comparable to the proposed adequacy criteria); (ii) the impact of public accessibility to the information, basically the adverse effects the information has on the data subject at present (comparable to the proposed context criteria); and, (iii) the relevance of the information on the individual's life, as in whether the information in question is of any present use to the individual or to the society with which he or she interacts (comparable to the proposed social relevance criteria). Additionally, he contemplates the use of the American 'substantial evidence standard' to complement the traditional 'proportionality test' used to determine the prevalence of opposing rights. Conversely, the Article 29 Data Protection Working Party released their "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) de Mario Costeja González" C-131/12" which adopts a different mechanism, based on a series of 'objective' questions. However, as mentioned earlier, we feel that an objective criterion would be unable to cover the complexity that often derives from right to be forgotten cases, however, we recognise such an objective approach could work as a preliminary assessment, or even perhaps a form of 'shortcut' or abbreviated procedure to rule over simpler cases where the request is focused on external elements of the content such as its the effects of time over its relevance.

All things considered, the Internet-connected society we live in demands that all action be taken with minimum delay, but with a great amount of care; after all, the transition into the world of bits has had an undeniably amplifying effect on many Constitutional rights, effectively constituting a right to a digital life on its own. With this in mind, the path ahead must be characterised by efficiency, measure and proportion, avoiding the paths that lead to unfair censorship or excessive leniency. The fact is that what happens in the world of bits has

[16] F. AHMED, *"Right to Be Forgotten: A Critique of the Post-Costeja González Paradigm" Academia.edu. Computer and Telecommunications Law Review*, Westlaw UK, Aug. 2015.

great repercussions in the world of atoms and, as such, we must pave the way for a generally recognised right to be forgotten.