Amicus Curiae Submission in the Case of *Da Cunha v. Yahoo de Argentina SRL*

A submission by the Open Society Justice Initiative to the Supreme Court of Justice of Argentina

March 2014

OPEN SOCIETY
JUSTICE INITIATIVE

IN THE SUPREME COURT OF JUSTICE OF ARGENTINA

Da Cunha v. Yahoo de Argentina SRL and Another

Expte. Nº 561/2010

I. INTRODUCTION

1. The Open Society Justice Initiative, a program of the Open Society Institute, an international non-governmental organization based in New York, U.S.A and various other offices around the world, represented by James A. Goldston, its executive director, and advised by Pablo Pejlatowicz, an attorney licensed to practice in Argentina, makes the following submission to this Honorable Court on the above referenced case.[1]

Object

2. The submission is made further to a request for leave to intervene in the current case as "friend of the court," filed by the Justice Initiative on 13 December 2013, pursuant to Acordada 07/2013 of this Court.

Facts and Procedure

3. The claimant, an Argentine model and musician, sued Yahoo Argentina and Google for damages and sought injunctions against search results of her name that produced links to several erotic and pornographic websites that used her name and photos without permission. She claimed that the two search engines were responsible for causing harm to her reputation, privacy and image rights.

4. In July 2009, a first instance court ruled in favor of the claimant.[2] In August 2010, an appeals court reversed the first instance judgment, two to one.[3] The majority found that, under general rules of tort liability, the search engines should not be held liable since the defendant failed to show that they acted with fault (*culpa*) in relation to third-party content. Only once an alleged victim notifies a search engine operator of links that violate her rights may the search engine become liable.

II. SUBMISSIONS

5. The case raises fundamental issues related, on the one hand, to the free circulation of information and ideas on the Internet and, on the other hand, to the need to protect individuals from harm resulting from online publications. We understand that it is the first time that such issues have reached this Honorable Court, and that there is also little jurisprudence on the topic in Latin America generally.

6. To assist the Court in its decision-making, this submission provides an overview of relevant comparative law from the European Union (E.U.) and the United States (U.S.) as well as arguments based on international human rights law and jurisprudence, including under the American Convention on Human Rights. For reasons of space, the main countries discussed within the E.U. are Germany, Spain and the United Kingdom.

7. This submission addresses three main issues: (a) the role of the intermediaries and their liability regimes in the United States and European Union; (b) whether search engines should be held liable for the content of their natural search results; and (c) whether search engines or other intermediaries should bear liability upon obtaining knowledge of unlawful publication.

A. The Role of Intermediaries

8. Intermediaries, including search engines, play an important role in facilitating access to online content. As a result, leading jurisdictions, including the U.S. and the European Union, have adopted special regimes exempting them from traditional publisher liabilities in relation to third-party content.

9. The development of the Internet has had a profound effect on human communication, providing a platform that grants billions of people around the world access to an unprecedented amount and diversity of information and ideas, regardless of frontiers.[4] At the same time, the Internet has enabled and empowered ordinary people to disseminate information and share their own ideas with a potentially global audience. Within a few decades, users worldwide have developed a "significant reliance on the Internet as an essential tool for their everyday activities."[5]

10. International human rights bodies, among others, have acknowledged the Internet's potential to further democratic values, noting that "[i]n light of its accessibility and its capacity to store and communicate vast

amounts of information, the Internet plays an important role in enhancing the public's access to news and facilitating the dissemination of information generally."[6]

11. Information location tools, such as search engines, play a crucial facilitating role in the online environment by helping web users locate and retrieve relevant information within the "vast library" of the world wide web. As one commentator put it, "without search engines, the Internet would be an endless expanse of digital babble, and finding any particular piece of information would be akin to locating a specific grain of sand in the Sahara Desert."[7] It is, indeed, hard to imagine an average Internet user that does not use a search engine or similar tool with some regularity. It was recently reported that a brief, 10-minute outage of various Google services caused a 40 percent dip in worldwide internet traffic.[8]

12. The same can be said of other Internet intermediaries, a general term that refers to various online service providers that facilitate user access to third-party content and services. In addition to information location tools, intermediaries include Internet service providers (who give users physical access to the Internet), hosting services (such as those that allow users to set up individual blogs or buy server space, like the photo-blogging platform Fotolog), and social network platforms (like Facebook or Twitter), among others.[9] Like telephone and telegraph lines and exchanges in the pre-digital world, Internet intermediaries are essential to the ability of users everywhere to communicate, and access the wide variety of services available, online.

13. For these reasons, many countries in the democratic world, including the European Union and the United States, have adopted special legal frameworks that limit the criminal and especially civil liabilities of intermediaries for infringements committed by their users or customers without any involvement by the intermediaries (other than through mere passive facilitation of the communications).

U.S. and European Models of Intermediary Liability

14. *United States*. The U.S. was the first country to adopt such a legal regime through section 230 of the 1996 Communications Decency Act (CDA),[10] which limits the liability of "interactive computer service" providers and users.[11] First, the Act establishes a presumption that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another

information content provider."[12] A second provision exempts intermediaries from liability as a result of "any action voluntarily taken in good faith to restrict access" to objectionable or unlawful material.[13]

15. U.S. lawmakers invoked three arguments for exempting Internet intermediaries from the traditional rules of publisher liability. First, given the volume and nature of online communications, Congress was concerned that intermediaries would engage in substantial "private censorship" of user content if they were to be held strictly liable for facilitating its publication. Secondly, they needed to address the paradox that whenever a host site took voluntary steps to try and limit offensive comments, they became more likely to be deemed to have exercised editorial control under traditional common law rules, creating a perverse incentive for intermediaries not to engage in any kind of self-regulation, which would be preferable to statutory intervention. Thirdly, U.S. lawmakers feared that strict liability for intermediaries would greatly hamper digital innovation, in part because small start-up platforms (the future engines of the digital revolution) would lack the resources to shoulder the resulting legal liabilities.[14]

16. The result of CDA section 230 has been to shield intermediaries from practically any cause of action related to third-party infringements. The only exception is copyright infringement, which is governed by a separate legal regime under the Digital Millennium Copyright Act (DMCA). The DMCA sets up a "notice and takedown" system, whereby intermediaries are required to take down infringing material (that they have control over) after being notified by a legitimate rights holder. The Act sets forth detailed procedures for notification, takedown as well as counter-notification of the original poster and possible reinstatement of the material.[15]

17. *European Union.* Motivated by similar considerations, in 2000 the E.U. adopted the Electronic Commerce Directive (ECD), which established "harmonised rules" for all member states on a range of issues affecting electronic communications, including "limitations of liability of intermediary service providers."[16] The Directive is binding on the member states, although they enjoy a degree of discretion in deciding how to implement its provisions through national legislation.

18. Section 4 of the Directive outlines the main exemptions from liability for intermediary service providers, dividing them into three separate categories. Article 12 creates a *mere conduit* exemption from any legal

liability for any service that consists essentially of transmission of third-party information, without any interference with its content (the telephony model).

19. Article 13, the *caching exemption*, applies to providers engaging in the *temporary* storage of information "for the sole purpose of making more efficient the information's onward transmission."[17] Many providers, including search engines, use caching for efficiency reasons, since it is not practically possible, for example, to conduct a real-time time search of the entire world wide web. Several conditions must hold for this exemption to apply, including that the provider must not "modify the information" and must update or remove it when so required by the original host or "a court or an administrative authority."[18]

20. Article 14 sets forth the *host exemption*: it conditionally exempts from liability any hosting provider whose service "consists of the *storage* of information provided by a recipient of the service," so long as the provider (a) "does not have actual knowledge of illegal activity or information" and (b) "acts expeditiously to remove or to disable access to the information" once it "obtain[s] such knowledge or awareness."[19]

21. Another central tenet of the ECD, which logically complements the liability limitations, is the principle that intermediaries (including mere conduit, caching and hosting providers) are under *no "general obligation … to monitor* the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity."[20]

22. Finally, it should be noted that, unlike the U.S. DMCA, the ECD does not contain any detailed procedures for the notification and takedown of illegal content; this was left to the regulation of each member state.

B. Search Engines Not Liable for Content of Natural Search Results Including "Snippets"

23. Search engines are not held liable for the content of natural search results in any of the jurisdictions covered in this brief. In some of these countries, they have been granted the same statutory protection as hosts or mere conduit operators (as these terms are defined by the ECD). In others, their precise categorization in law remains somewhat unclear, but courts have nevertheless granted them immunity in relation to third-party content appearing in their natural search results.

24. Natural search results are the results generated by a search engine in direct response to a user search query. They normally produce a list of hyperlinks to third-party content, followed by a short description of the

content on the referenced website (known as a "snippet"). The search results considered defamatory by the claimant in the current case involve natural search results. These are to be distinguished from the advertising-related hyperlinks produced by the search engine in response to a user query, such as the highlighted links found at the top and right side of the natural search results on a Google search, which are labeled as "advertising."

Court of Justice of the European Union

25. The case law of the Court of Justice of the European Union strongly suggests that search engines are entitled to liability exemption under the ECD in relation to their natural search results.

26. In *Google France v. Louis Vuitton*,[21] the Grand Chamber of the Court of Justice of the European Union (CJEU) considered whether a search engine ought to be held liable for advertising-related links that violated the trademarks and other commercial interests of the French luxury brand. Even though the case did not involve natural search results, but paid commercial links, the CJEU holding is instructive for the current case.

27. The illegal content at issue in this case involved AdWords, a Google service whereby Google sells "keywords" to advertisers, whose ads appear whenever a user within the relevant jurisdiction includes the respective keywords in her search term.[22] The first question before the CJEU was whether search engines can benefit from any of the limitation of liability provisions of the ECD given that, as indicated above, the ECD does not explicitly regulate the liabilities of search engines. Relying on recital 42 of the preamble to the ECD, the Court held that a search engine (or any other "information society service provider") enjoys liability limitation under the ECD if its activities are "'of a mere technical, automatic and passive nature,' which implies that that service provider has neither knowledge of nor control over the information which is transmitted or stored."[23]

28. The Court noted that a search engine does not lose its ECD intermediary protection merely because it is engaging in profit-making activity or setting the terms of advertising payments. Furthermore, the fact that it operates a keyword system does not "of itself" mean that the search engine has control over the data entered into its system by advertisers and stored in memory on its server. The Court contrasted those actions with

the role played by the search engine (if any) "in the drafting of the commercial message which accompanies the advertising link" or in the selection of keywords, which *might* involve something more than a neutral or passive intermediation.[24]

29. This reasoning demonstrates that the role of a search engine in relation to natural search results would in principle be entitled to intermediary protection under the ECD, considering that, by their nature, natural searches are closer to a "technical, automatic and passive" activity than the (automatic) selling of advertising terms by the search engine. In natural search, the results are determined by the user query and the content within those results (snippets) is provided by third parties, with the search engine providing what is essentially a cataloguing service.

European Court of Human Rights

30. The ECHR has not ruled directly on questions of search engine liability. However, its case law includes helpful clarifications on the nature of hyperlinks, which is what search results are in essence.

31. In *Swiss Raelian Movement v. Switzerland*,[25] the ECHR reviewed the refusal of local police authorities to grant permission to the applicant to conduct a poster campaign in public spaces involving a poster promoting a "message from Extraterrestrials" and including the organization's website address. The Swiss authorities argued that the the Movement was engaged in activities that were immoral and contrary to public order, and that its website contained links to a separate site promoting human cloning, which is illegal in that country. A divided (9-8) Grand Chamber of the Court held that there had been no violation of Article 10, finding that the expression at issue was "closer to commerical speech" on public space.[26]

32. In several joint opinions, the dissenting judges pointed out that the Movement's website had not been banned.[27] With respect to the hyperlink to the cloning site, three of the dissenters argued that "there are a number of independent decisions to be taken by" a person clicking on a hyperlink and that attributing responsibility to the provider of the hyperlink requires "careful analysis":

> "A reference is not an endorsement or an identification... Otherwise the "referring" person would be obliged to distance himself all the time and that would impose a considerable burden on freedom of speech in the world of the Internet. A hyperlink certainly facilitates the dissemination of an idea … but

not all dissemination gives rise to responsibility. As the Supreme Court of Canada held in a defamation case, hyperlinks are essentially different from publication and are by themselves content-neutral. Like references, they communicate the existence of something, but do not, by themselves, communicate its content (*Crookes v. Newton*, 2011 SCC 47)."[28]

Germany

33. Recent case law of the German Supreme Court (Bundesgerichtshof, BGH) has settled the question of search engines' civil liability for natural search results, finding no liability. The German law giving effect to the ECD did not make any specific provisions for search engines or hyperlinking, leaving open the question of their status as intermediaries. In two copyright infringement cases, known as *Vorschaubilder I* and *Vorschaubilder II*, a photographer sued Google for, inter alia, copyright infringement claiming that pictures he had taken of a German celebrity and posted on his website showed up as thumbnails in a Google Images search.[29]

34. *Vorschaubilder I* was decided primarily on copyright grounds, based on the doctrine of implied consent.[30] Importantly, however, the BGH also noted that even if the photographer had not implicitly consented to such reproduction, Google would have been exempt under ECD Article 14 (the "host" provision) because the image search was merely a technical, automatic, and passive activity that produced results over which Google had no control and about which Google could not have had prior knowledge. As per the terms of the Directive, Google could only be held liable for copyright infringement if and once it obtained knowledge of illegal content and did not expeditiously remove said content. The BGH explicitly relied on the CJEU's *Louis Vuitton* ruling in its reasoning.

35. *Vorschaubilder II*,[31] handed down one year later, reaffirmed *Vorschaubilder I* but also went further. The BGH emphasized that, since Google returned image results in a passive and automatic manner, it had no sure way of differentiating between images published by legitimate right holders and those published by unauthorized third parties. Moreover, the right holder would not be left without recourse as he always had the option of bringing a legal action against the original copyright violator.

36. The rationale of the top German court applies even more forcefully to the current case since copyright disputes tend to be legally less complex, and constitutionally less weighty, than questions of defamation or privacy law.

Spain

37. The Spanish legislature has implemented the ECD by specifically extending the "hosting" protection to search engines, thus exempting them from liability for third-party violations.[32] In addition, Spain adopted a strict definition of "actual knowledge" – as a trigger for the duty of intermediaries to disable access to infringing content expeditiously – which generally requires a declaration by a "competent body" that the publication is unlawful, or an order from such a body directing the intermediary to remove the information.[33]

38. A case quite similar to the current one was decided by the Madrid Court of First Instance in *Palomo v. Google Inc*.[34] The claimant argued that Google was responsible for providing, in natural search results, hyperlinks to sites carrying content that defamed him. The Spanish court rejected Palomo's claims, taking notice of the European trend that fails to impose a general obligation on intermediaries to monitor the legality of the communications they facilitate. In the absence of actual knowledge, as defined above, Spanish law provides for "exoneration from responsibility" for those offering intermediary services.

39. The first instance judgment was confirmed on appeal by the Madrid Court of Appeals. The appeal court further elaborated on the "actual knowledge" requirement, finding that only notification to Google of a court judgment determining that the information at issue was illegal would have placed the search engine on notice under Spanish law and/or required it to remove the content.[35]

United Kingdom

40. British courts have held that search engines are not liable for natural search results, and in fact cannot even be considered "publishers" of third-party content appearing in such results.

41. The UK did not make any special provision for search engines in the act implementing the ECD.[36] On the question of actual knowledge, Regulation 22 of the act stipulates that "in determining whether a service provider has actual knowledge for the purposes of [the caching and host exemptions], a court shall take into

account all matters which appear to it in the particular circumstances to be relevant," including whether the service provider has received any complaints by aggrieved parties pursuant to procedures established by the Regulation for that purpose.

42. The most relevant UK ruling for the present case is *Metropolitan v. Designtechnica and Google, Inc.*,[37] which was decided by the High Court of Justice on common law grounds, rather than based on the ECD.[38] As in the current case, the claimant argued that Google was liable for defamatory statements hosted by a third site (Designtechnica) that appeared on natural search snippets whenever a search for the claimant's name was conducted.

43. The British court held that Google was not liable for the defamatory content at issue because the search engine could not be considered a "publisher" of such content at common law.[39] First, the court noted, a Google search involves "no intervention on the part of any human agent" and is instead a passive act performed "by the web-crawling robots." The court compared the online search process to "a search carried out in a large conventional library," with the search engine merely playing "the role of a facilitator."[40]

44. Secondly, the court turned to the question of control, noting the important difference between search engines and traditional hosts that directly store unlawful content on their servers: unlike hosts, it is not possible for a search engine operator to "merely press a button to ensure that the offending words never reappear on a . . . search snippet" since it has "no control over the search terms typed in by future users."[41] Since Google cannot be considered a (re-) publisher of third-party content, it cannot be said that Google "authorized or acquiesced" in the continued appearance of the defamatory snippet in its search results.[42] Search engines therefore cannot be held liable at common law for defamatory "snippets" even after the search engines have been informed of such content.[43] Notification or actual knowledge does not in any way change the nature of search engines' liability.

United States

45. Attempts to circumvent section 230 of the Communications Decency Act (CDA), which grants online intermediaries full immunity over third-party publications (other than on copyright matters),[44] have failed in virtually all cases in the United Stated. Search engines are no exception. In *Parker v. Google, Inc.*[45] a

federal district court held that Google was not liable for archiving and caching defamatory comments about the plaintiff that were posted on a third-party website.[46] Citing an established line of precedent, the court argued that the "intent of [section 230] is to preclude courts from entertaining claims that would place a computer service provider in a publisher's role," and that Google was therefore immune from "state tort claims" such as defamation and invasion of privacy.[47]

46. While *Parker* addressed basic functionalities of the search system such as archiving and caching related to natural search results, more advanced features of internet search systems have also been found immune. In *Goddard v. Google, Inc.*,[48] a federal district court found Google not liable for content generated by its Keyword Tool, which allegedly "employ[ed] an algorithm to suggest specific keywords" like "free ringtone."[49] The claimant argued that Google knew, or should have known, that its Keyword Tool generated such terms that "materially contributed" to fraud in the mobile subscription service industry.[50] However, the court found mere knowledge to be insufficient. The "Keyword Tool [was] a neutral tool,"[51] the court held, even if Google was "aware of fraud in the mobile subscription service industry and yet disproportionately suggest[ed] the term 'free ringtone'",[52] the Keyword Tool did nothing more than "provide options that advertisers may adopt or reject at their discretion."[53]

Conclusion

47. The major jurisdictions analyzed in this brief have, at the very least, exempted search engine operators from civil liability over third-party content that appears *in their natural search results*. This position stems, in large part, from an acknowledgment that search engine operators are under no general duty to monitor the legality of the entire universe of online information indexed by them, which would be a practically impossible task anyway. Courts and legislators have also recognized the severe adverse effects that a strict liability regime for search engines would have on the ability of web users to access and exploit the extraordinary wealth of information and ideas on the Internet.

48. The specialized international mandates on freedom of expression reached the same conclusion, treating searching as "mere conduit:"

"No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so ('mere conduit principle')."[54]

C. Does Notice Trigger Liability for Search Engines and/or a Duty of Removal?

49. A second set of questions raised by this case involve whether search engines may be exposed to potential liability for continued publication following notification by an aggrieved party of allegedly unlawful third-party content appearing in their search results.

50. To answer that complex question—on which there is no clear consensus in comparative law—we start by describing, first, the applicable legal regimes, and the key criteria developed by legislators and courts, in the European Union area and the United States. The second part of this section discusses how general principles of international human rights law should be applied in this context, given also the paucity of international jurisprudence directly on point.

European Union Jurisdictions

51. Whether a search engine in European Union countries may be liable for continuing to provide results and links to a given site, after it has been notified that it contains allegedly unlawful content, would depend firstly, on how the national legislature, or a national court hearing a specific case, characterizes the nature of a search engine activity or operation; and secondly, on what form of notification (or other proof of knowledge of the unlawful content) is required.

52. In terms of the classification of the search engine's activity, under the ECD it might be classified as (a) mere conduit or caching, (b) hosting, or (c) neither. Mere conduit and caching services are not subject to takedown obligations under the ECD, and should not, in principle, assume any liabilities even upon notification. Hosts assume liability upon obtaining "actual knowledge" of the illegality, if they do not act "expeditiously" to disable access to the infringing content.[55] Finally, if a competent national authority

decides that search operations do not fit under any of the three ECD categories, it would be free to apply traditional rules of civil liability for unlawful publication or dissemination.

53. Two other crucial elements of post-notification liability are "actual knowledge" and (private or *ex parte*) notification requirements. The practice of EU member states is not uniform on these two questions, [56] but it does identify some of the key factors European courts take into account in deciding questions of post-notice liability.

54. *Actual Knowledge*. If a search engine is deemed to have acted as a host in the circumstances of the case, the next question under the ECD would be whether (and when) it obtained "actual knowledge" of the illegal content at stake. The ECD does not define the concept of "actual knowledge," leaving it to the interpretation of the various member states.

55. The case law of the Court of Justice of the European Union sheds, however, some light on the nature of the "actual knowledge" requirement. The Court has made clear that not every private notice or complaint will be sufficient to establish actual knowledge: "a [private] notification admittedly cannot automatically preclude the exemption from [host] liability…, given that notifications of allegedly illegal activities or information may turn out to be *insufficiently precise or inadequately substantiated*."[57] The Court went on to note that "such notification represents, as a general rule, a factor of which the national court must take account when determining … whether the [host] was actually aware of facts or circumstances on the basis of which a diligent economic operator should have identified the illegality."[58]

56. Notifications or injunctions issued by a court or another competent public authority are generally assumed to put the service provider on notice for ECD purposes. As already noted (in para. 38), under Spanish law only a "competent body" can put an intermediary on notice for the purposes of the ECD, thus ruling out private complaints. In Portugal, where the law also requires notification by a judicial authority, practice appears to have developed an additional model: a limited exception that allows for non-judicial notice for "manifestly illegal content," such as child pornography, racist or terrorist material.[59]

57. *Notification Requirements.* In those countries that consider *private* notice sufficient, most jurisdictions, including France and the UK, specify the requirements that a notification must meet to amount to "actual

knowledge." In France, for a notification to be valid, it must include details such as the full identity of the notifying party, the date and precise location of the purportedly illegal information, and the legal basis for the complaint.[60] The purpose of these requirements is to discourage frivolous or abusive complaints and allow intermediaries to make informed decisions about content takedown.

58. Notification requirements may be even more onerous when it comes to requests for taking down content in certain specific contexts, such as defamation. A recently adopted defamation law for England and Wales regulates the liabilities of website operators "in respect of a statement posted on the website." With respect to third-party content, website operators are liable only if (a) "it was not possible for the claimant to identify the person who posted the statement" and (b) the operator failed to comply with a notice of complaint.[61] Details of the notification requirements have been developed by the Ministry of Justice, which has published a draft Defamation (Operators of Websites) Regulations 2013.[62] Under Sec. 5 of the Act and the proposed regulations, a defamation claimant would have to include several detailed elements in a notice of complaint to a website operator.[63]

United States

59. The complete immunity granted to intermediaries in the U.S. by section 230 CDA—with the exception of copyright infringement—is not affected by, or subject to, any notification by the aggrieved party.[64] As indicated, a different legal regime governs intermediary liability for copyright-infringing material under the DMCA, which provides for a counter-notice to the original poster, but only after content has been taken down. However, if the poster objects to the takedown, the host must put back the material within 10 business days, unless the complainant notifies the host that they have filed a court action seeking an injunction against the re-posting of the material.[65]

The Problem of "Private Censorship" and the Need to Guarantee User Rights

60. The removal of user-generated content by Internet intermediaries at the request of private parties (individuals, corporations etc.) raises serious questions for freedom of expression in the Internet age, including concerns over "private censorship." Traditionally, private publishers of media and other content have enjoyed broad freedom in deciding who and what to publish in their platforms. This corresponds to a

legal regime that, with few exceptions, holds them liable for the legality of their publications, including content authored by others.

61. The advent of the internet has radically changed the relationship between the new breed of "publishers" (hosts and platform operators) and the providers and consumers of the wealth of information and ideas available online. On the one hand, the web has greatly simplified and democratized the ability of individuals and groups to cheaply disseminate information of all kinds and broadcast their views to a large audience. On the other hand, there is an unprecedented level of concentration of control, partly as a result of the network effect: much of the information available online is hosted, located or ultimately controlled by a relatively small number of privately-owned global or national platforms. These new "sovereigns of the cyberspace" exercise therefore, at least in theory, an extraordinary amount of power over the free circulation of online content worldwide. The same holds true even with respect to smaller operators, for example at national or local level, as the online publishing platforms are generally controlled by a finite number of private operators. Even the widely-read individual blogger or investigator – the archetype of the new "citizen journalism" – must purchase space on some server willing to host and maintain her blog.[66]

62. International human rights law prohibits, or greatly restricts, government measures aimed at preventing information and ideas from reaching the public in the first place (prior restraint). The American Convention on Human Rights does so in particularly strong terms, providing that "the exercise of the right [to freedom of thought and expression] shall not be subject to prior censorship".[67] With respect to the Internet, however, private controls over what content stays online, and what is taken down (or rendered inaccessible), are at least as important—or potentially insidious—as government censorship.

63. The American Convention specifically prohibits such private interference as an "indirect restriction" on free expression: it prohibits "the abuse of government *or private controls* over newsprint, radio broadcasting frequencies, or equipment used in the dissemination of information, or by any other means tending to impede the communication and circulation of ideas and opinions."[68] Servers, bandwidth and digital bytes are the newsprint of the current era.

64. Read together with Article 1(1) of the Convention—which requires state parties "to ensure to all persons subject to their jurisdiction the free and full exercise of [the Convention] rights and freedoms"—this

interpretation of Article 13 requires states to adopt positive measures, through legislation and other means, to prevent, and create remedies against, the arbitrary silencing of internet users by private operators.

65. This general principle has also been endorsed by other international human rights mechanisms. The U.N. Human Rights Committee has affirmed that Article 19 ICCPR "requires States parties to ensure that persons are protected from any acts by private persons or entities that would impair the enjoyment of the freedoms of opinion and expression to the extent that these Covenant rights are amenable to application between private persons or entities."[69]

66. A case currently pending before the CJEU touches on related questions of private censorship. It involves a "right to be forgotten" complaint against Google Spain brought by a Spanish citizen, who asked the search engine to refrain from including in its search results links to an old newspaper article that contained unfavorable information about the claimant.[70] In a June 2013 opinion on the case,[71] Advocate General Jääskinen concluded that the original publication at issue was lawful and therefore not subject to the 'notice and takedown' provisions of the ECD, which apply to illegal content. He went on:

> "I would discourage the Court from concluding that these conflicting interests [between free speech and privacy] could satisfactorily be balanced in individual cases on a case by case basis, with the judgment to be left to the internet search engine service provider. … This would entail an interference with the freedom of expression of the publisher of the web page, who would not enjoy adequate legal protection in such a situation... It would amount to the censuring of his published content by a private party."[72]

67. Internet users' free speech rights need to be carefully reconciled with the rights of other individuals as well as the right of private operators to conduct business without excessive or unreasonable interference. However, traditional notions of "publisher control" are often ill-suited to the Internet environment. Considering, for example, the facts of the current case, Google is no more a "publisher" of its natural search results than a physical library is the publisher of the books it catalogues in its index system. The U.S. and European regimes of limitations on intermediary liability were adopted precisely to avoid their becoming the new mega-censors of national or global content: for the intermediaries this entails giving up (some or most) editorial control in exchange for being exempted from the strict legal liabilities of traditional publishers.

68. *Due Process Requirements*. The extra-judicial removal of, or disabling of access to, user-generated content by online service providers raises important due process questions. Some authorities, including the international special mandates on free expression, have taken the position that "intermediaries should not … be subject to extrajudicial content takedown rules which fail to provide sufficient protection for freedom of expression (which is the case with many of the 'notice and takedown' rules currently being applied)."[73]

69. The core of the problem is that extrajudicial takedown regimes put the intermediaries in the role of gatekeepers, or arbiters of the legality of online expression, often across dozens of jurisdictions—a major responsibility for which they have neither the expertise nor the public confidence required to fulfill it. There is a strong argument to be made that such a role properly belongs to the courts, absent perhaps a need for urgent action to disable access to content that is exceptionally harmful and indisputably illegal (such as child pornography).

70. For all other disputes that do not fall in the latter category—including, arguably, most cases involving allegations of defamation or privacy infringement—the legal issues are too complex and the stakes for democratic debate too high to be left to private censorship. This also assumes that different takedown regimes may be needed for different forms of infractions: what works for pirated content or malicious software may not necessarily work for defamation, breach of privacy or threats to public order.

71. Conclusion. Some of the jurisdictions discussed in this brief, such as Spain and Portugal, have opted for a regime that, by and large, requires judicial authorization for online content removal. It is our submission that, in line with the international law principles described immediately above, this would be the most appropriate regime for complex disputes, involving constitutionally protected speech, in order to minimize private censorship and allow the courts to resolve such questions of importance for a democratic society. Special procedures for expedited judicial review may be established in order to undo or minimize unfair harm to claimants' interests where appropriate.

72. Others countries, such as the UK on defamation or the US on copyright infringement, are pursuing a sectorial approach, adopting special rules that allow for a degree of private takedown but with safeguards that seek to protect user rights and legitimate public debate. Such safeguards include duties to notify the original poster and the right of the poster to object to a takedown, or to request the reinstatement of his/her

content. Whenever there is a genuine dispute on the legality of the content at issue, it should be resolved by a court of law.

III. CONCLUSION

73. In conclusion, we respectfully urge this Honorable Court to find, in line with the virtually unanimous position in the democratic world, that (a) search engine operators are not liable for the content of their natural search results; and (b) that they should not be placed under a general duty to monitor third-party communications in order to prevent illegal publications in the future.

74. We additionally submit that, at least with respect to complex legal disputes such as those in the current case, search engines and other intermediaries should not be legally *required* to remove (or disable access to) third-party content unless and until ordered by a court to do so. In the alternative, a duty of takedown upon private complaint or notification should be accompanied by strong substantive and procedural safeguards that would adequately protect users, and the community at large, from the dangers of private censorship. Ideally, such a system should have a statutory underpinning, in the absence of which the first option (no duty of takedown) should be preferable.

James A. Goldston, Executive Director

Darian K. Pavli, Senior Attorney

10 March 2014

[1] The research assistance of Jodie Liu in the preparation of this submission is gratefully acknowledged.
[2] Juzgado Nacional de 1a Instancia en lo Civil Nro. 75, Judgment of 29 July 2009.
[3] Camara Nacionale de Apelaciones en lo Civil, Judgment of 10 August 2010.
[4] See *Reno v. ACLU*, 521 U.S. 844, at 853 ("The Web is …comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services. From the publishers' point of view, it constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers.")
[5] Council of Europe (Committee of Ministers) Recommendation (2008)6 on Measures to Promote Respect for Freedom of Expression and Information With Regard to Internet Filters.
[6] European Court of Human Rights, *Times Newspapers Ltd v. the United Kingdom* (Nos. 1 and 2), Judgment of 10 March 2009, para. 27. See also *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, Judgment of 5 May 2011.
[7] D. J. Solove, *The Future of Reputation: Gossip, Rumor and Privacy on the Internet*, 2007, Yale University Press, p. 9.

[8] "Google goes dark for 2 minutes, kills 40% of world's net traffic," *The Register*, at http://www.theregister.co.uk/2013/08/17/google_outage/. Even though Google offers various services, including email accounts, its search engine is by far the most widely used.
[9] OECD Paper on "The Role of Internet Intermediaries in Advancing Public Policy Objectives" (September 2011), at http://www.oecd-ilibrary.org/science-and-technology/the-role-of-internet-intermediaries-in-advancing-public-policy-objectives/internet-intermediaries_9789264115644-4-en.
[10] 47 U.S.C. §§ 151-621.
[11] The CDA defines "interactive computer service" as "any information service, system, or access software or provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions." Sec. 230(f)(2).
[12] Sec. 230(c)(1).
[13] Sec. 230(c)(2).
[14] See Electronic Frontier Foundation, "CDA 230: Legislative History," at https://www.eff.org/issues/cda230/legislative-history.
[15] 17 U.S.C. § 512. For a summary of how the DMCA regime works, see http://www.sfwa.org/2013/03/the-dmca-takedown-notice-demystified/.
[16] Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, In Particular Electronic Commerce, In The Internal Market (Directive on electronic commerce), available at http://ec.europa.eu/internal_market/e-commerce/directive/index_en.htm.
[17] Article 13(1), Directive 2000/31/EC.
[18] Ibid.
[19] Article 14(1) (emphasis added).
[20] Article 15(1) (emphasis added).
[21] Case C- 236/08, Judgment of 23 March 2010 (Grand Chamber).
[22] The order in which the advertisers appear in the search results depends, among other factors, on the AdWords fee they have paid the search engine operator. The selection and purchase of AdWords by advertisers may be done electronically, i.e. without any human intervention by search engine employees.
[23] Para. 113.
[24] Paras 117-18. The Court did not make a conclusive finding on the merits of the case: this being a preliminary ruling on referral by the French Cour de cassation, the role of the CJEU was to answer questions of general application of EU law posed by the French court, leaving to the domestic court their application to the facts of the case.
[25] Judgment of 12 July 2012 (Grand Chamber).
[26] Para. 62 et seq.
[27] Joint Dissenting Opinion of Judges Tulkens, Sajó, Lazarova Trajkovska, Bianku, Power-Forde, Vučinić and Yudkivska, para. 11.
[28] Joint Dissenting Opinion of Judges Sajo, Lazarova Trajkovska and Vucinic, at III.
[29] A Google Images search is similar to a traditional natural search in that it produces images of a person, object etc found on the web in response to a user query; the user may use a regular query (formulated in words) or upload another image as a search query.
[30] BGH judgment of 29 April 2010, I ZR 69/08, available at https://openjur.de/u/32421.html. The BGH determined that, since the user had uploaded images of his copyright-protected work without taking any measures to prevent those images from showing up in search engine image results, the user had impliedly consented to the reproduction of the image as a thumbnail preview in a Google Images search.
[31] BGH judgment of 19 October 2011, Az. I ZR 140/10 (Vorschaubilder II), available at http://openjur.de/u/270380.html.
[32] Law 34/2002, Ley de Servicios de la Sociedad de la Informacion y de Comercio Electronico, at http://noticias.juridicas.com/base_datos/Admin/l34-2002.html.
[33] Ibid., art. 17(1).
[34] Judgment of 13 May 2009.
[35] Audiencia Provincial of Madrid, 9th Section, 19 February 2010, Judgment 95/2010, at http://audiencias.vlex.es/vid/-220093371.
[36] The Electronic Commerce (EC Directive) Regulations 2002.
[37] [2009] EWHC 1765 (QB), available at http://www.bailii.org/ew/cases/EWHC/QB/2009/1765.html.
[38] The British court resolved the case exclusively on common law grounds in part because it found that neither the ECD, nor the British implementing Regulation of 2002 expressly extended host protection to search engines. The *Metropolitan* judgment preceded the *Louis Vuitton* ruling of the CJEU, which found that search engines are "information society service providers" within the meaning of the ECD, which might be entitled to host protection depending on the nature of the specific conduct at issue.
[39] Ibid at 53.

[40] Ibid (internal quotations omitted).
[41] Ibid at 55. The Court acknowledged that Google can block certain content from appearing in its search results but that it is only able to do so if provided with a specific URL; a broader blocking measure is not possible without excluding at the same time "a huge amount of other material which might contain some of the individual words comprising the offending snippet." Ibid. at 57. A more effective solution would be for the original poster of the illegal content to (be forced to) either remove such content altogether or alter the code of its own website so that is not picked up by a search engine's crawlers.
[42] Ibid at 55.
[43] Ibid.
[44] See paras 17-19 above.
[45] 422 F. Supp. 2d 492 (E.D. Pa. 2006), decision summary aff'd, 242 Fed. App. 833 (3d Cir. 2007), cert denied 522 U.S. 1156 (2008).
[46] Ibid at 501.
[47] Ibid (internal citations and quotations omitted).
[48] 640 F. Supp. 2d 1193 (N.D. Ca. 2009).
[49] Ibid at 1197.
[50] Ibid. ("Plaintiff contends that the suggestion of the word 'free,' when combined with Google's knowledge 'of the mobile content industry's unauthorized charge problems,' makes the Keyword Tool 'neither innocuous nor neutral.' (Pl.'s Opp. At 7) . . . Plaintiff's argument that the Keyword Tool 'materially contributes' to the alleged illegality does not establish developer liability.")
[51] Ibid at 1198.
[52] Ibid at 1197.
[53] Ibid at 1198.
[54] 2011 Joint Declaration of the United Nations Special Rapporteur on Freedom of Opinion and Expression; the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights (IACHR); the Organization for Security and Cooperation in Europe (OSCE) Representative on Freedom of the Media; and the African Commission on Human and Peoples' Rights (ACHPR) Special Rapporteur on Freedom of Expression; at http://www.oas.org/en/iachr/expression/showarticle.asp?artID=848&lID=1, at 2(a).
[55] This assumes that hosts also have the practical ability to take down, or disable access to, any third-party material stored in their own servers; in the case of a search engine disabling access tends to be a more complex matter because the material is normally hosted elsewhere.
[56] For a summary of EU trends on this issue, see Verbiest, note 37 above, p. 14.
[57] *L'Oreal v. eBay*, Case C-234/09, Grand Chamber Judgment of 12 July 2011, para. 122 (emphasis added).
[58] Ibid. Advocate General Jaaskinen presented similar arguments in the same case: "First, it is evident that the service provider must have actual knowledge of, and *not a mere suspicion or assumption* regarding, the illegal activity or information. It also seems to me that legally 'knowledge' may refer only to past and/or present but not to the future. … Secondly the requirement of actual knowledge seems to *exclude construed knowledge*. It is not enough that the service provider ought to have known or has good reasons to suspect illegal activity. This is also in line with Article 15(1) of [the ECD] which forbids the Member States to impose on service providers general obligations to monitor the information they transmit or store or to actively seek facts or circumstances indicating illegal activity." Opinion of 9 December 2010, para. 162-163 (emphasis added).
[59] European Commission, "Summary of the results of the Public Consultation on the future of electronic commerce in the Internal Market and the implementation of the Directive on electronic commerce (2000/31/EC)", p. 10.
[60] Law No. 2004-575, note 36 above, art. 6-I(5).
[61] Defamation Act 2013, sec. 5(3), at http://www.legislation.gov.uk/ukpga/2013/26/section/5/enacted.
[62] The draft is not final; it is currently subject to public consultation, at http://www.olswang.com/media/29576493/defamation_bill_section5_regulations.pdf. Once approved by the Ministry of the Justice, it must be ratified by Parliament.
[63] These include: the name and email address of the complainant; the URL or location of the statement complained of; an explanation of what the statement says and why it is defamatory of the complainant; the meaning the complainant attributes to the statement complained of; the aspects of the statement which the complainant believes are factually incorrect or opinions not supported by fact; confirmation that the complainant does not have sufficient information about the author to bring proceedings against them; and confirmation of whether the complainant consents to his name and email address being provided to the poster. For additional details on the operation of the notification system and its implications, see Ashley Hurst, "The Section 5 Defamation Act Regulations: A complex red herring," at http://inforrm.wordpress.com/2013/08/16/the-section-5-defamation-act-regulations-a-complex-red-herring-ashley-hurst/
[64] In the seminal case of *Zeran v. America Online*, a federal circuit court held that the host of an internet message board was not liable for third-party defamatory messages appearing on the board. Being put on notice did not change its legal position. Rejecting the argument that section 230 created immunity only for "publishers" of defamatory comments and not for "distributors" who had "acquired knowledge of the defamatory statements' existence," the Fourth Circuit held that distributor

liability is "merely a subset, or a species, of publisher liability, and is therefore also foreclosed by § 230." Imposing "liability upon notice", the court explained, would defeat the dual purposes advanced by section 230 of the CDA to reduce "service providers' incentives to restrict speech and abstain from self-regulation.

[65] DMCA sec. 512.

[66] For example, in the wake of the disclosure by the Wikileaks organization of classified U.S. government data, various providers, including Amazon hosting services and online payment conduits Paypal and Mastercard, cut off their service to Wikileaks.org. See John Naughton, "WikiLeaks row: why Amazon's desertion has ominous implications for democracy," *The Guardian*, 11 December 2010.

[67] Art. 13(2). The only exception permitted by the Convention is the statutory regulation of entertainment venues "for the sole purpose of regulating access to them for the moral protection of childhood and adolescence." Art. 13(4).

[68] Art. 13(3).

[69] General Comment No. 34, 12 September 2011, para. 7, at http://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf.

[70] Case C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja Gonzáles* (undecided). The original publication, involving the claimant's mortgage delinquency, was truthful and in fact required by Spanish law. However, the claimant argued that its ongoing publication violated his right to personal data protection under EU and Spanish law.

[71] Opinion of the Advocate General, 25 June 2013, at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=138782&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=960253.

[72] Ibid, paras 133-134.

[73] 2011 Joint Declaration of the UN, OAS, OSCE and ACHR special mandates on free expression, para. 2(b). The declaration does not specify what would constitute "sufficient protection" for free expression in this context.