Global Freedom of Expression
@ COLUMBIA UNIVERSITY

"Are Courts re-inventing Internet Regulation?"

Dr. Agnes Callamard
Director, Global Freedom of Expression @Columbia University
Discussion Paper[1], May 2015

INTRODUCTION

The debate on Internet governance, and freedom of expression on-line in particular, has largely focused on the place of Internet technology itself in the various regulatory framework and principles. The infrastructure of its hardware, the design of its software and a range of other elements altogether form the cyberspace or the digital world within which human beings connect, inform, communicate, sell and buy, and also harm each other. All technological components (hardware, software, nodes, etc.) are potentially matters for regulation[2], which greatly impacts on the governance of the Internet, and the protection of human rights and freedom of expression on-line. It is easy to see why for many years technology was seen and construed as *determining* Internet governance and regulation, on-line values and norms, particularly in view of the relative weaknesses of other actors, states included, in the earlier days of Internet governance. This state of affairs has progressively, and then rapidly, evolved with every few years bringing different actors, and shifting divisions of power and responsibilities amongst them. The original model of a cyber-world governed by the technologist or engineer and (some) users has morphed into an incredibly complex array of actors whose interaction and relative power with regard to Internet governance are the objects of much debate amongst academics, policy makers and practitioners alike.

This paper introduces an actor, which has been neglected so far by those analyzing the forces shaping the Internet world and founding its normative system(s), namely the Tribunals – national or regional judges and courts. It is part of a larger research[3] into understanding the formation of global norms on freedom of expression and information (FoE/I) in an era defined and dominated by information, asking whether we are witnessing the emergence of an inter-meshed legal global system for freedom of expression and

[1] An initial version of this paper was written for and presented at the "Justice for Free Expression" Conference, organized by Global Freedom of Expression @Columbia, on March 10-11, 2014. This remains a discussion paper and a draft. I will very much welcome and value comments and critiques, suggested readings or additional court cases I should consider: ac3699@columbia.edu

[2] The primacy or centrality of technology remains a key feature of the Internet governance literature. See for instance Laura de Nardis who defines the first tasks of internet governance as the "design and administration of the technologies necessary to keep the internet operational and the enactment of substantive policies around these technologies" in **The Global War for Internet Governance,** Yale University Press, 2014, p.6

[3] One key project involves monitoring, analyzing and cataloguing court cases from around the world, to determine whether legal precedents are emerging and morphing into global norms. A database of court cases will be launched in May with initially some 200 cases from around the world. For further information on the initiative, please check: www.globalfreespeech.columbia.edu.

information, guided by common norms[4].

This discussion paper argues that judicial ruling over matters of on-line freedom and Internet governance are becoming highly influential – not just as interpreters of the law(s) (the tribunals traditional function) but as shapers or transformers of Internet norms and values. This evolution has become particularly clear over the last year or two, with 2014 constituting a watershed, demonstrating the increasing confidence of judges and Tribunals in challenging engineers, users, corporations, or indeed governments (at least in countries where the independence of the Judiciary is respected) and possibly establishing different norms as far as the cyberspace is concerned.

I - On State and Geography

There is little doubt that technology accounts for the "trans-boundary, geography-defying quality"[5] of on-line expression, to use Daniel Bethlehem's expression. Human agencies' interaction with technology has solidified its geography-defying reach to create a global communication and information system for the 21st Century.

As scholars and cyber activists have repeatedly emphasized, the State was originally not one of those agencies. Other actors founded what can be described as the "post-Westphalian"[6] Internet world. However, there is difference of opinion as to whom or what has exercised the greatest influence, besides Technology itself.

For some scholars, the primary characteristic of cyberspace is *decentralized individual action*[7], engaged in non-market and peer production of information; ultimately creating a networked information economy[8] whose territory and modus operandi defy geography.

For others, *transnational institutions* have played the critical role in fostering the Internet's global governance, with *networked governance* bridging thus the gap between national institutions and global connectivity[9].

For others again, it is principally *corporate actors* who are driving the global, geography-defying nature of Internet governance, a hegemony reflected in more recent years in the privatization[10] and commoditization of the Internet, and, in what Tim Wu has described, as its "cartelization"[11].

Altogether, these actors, alone, in alliance or in competition with each other, and always in interaction with the technology, are said to be defining Internet and on-line freedom. They have done so by going beyond the primacy of the Nation-State and beyond the Westphalian

[4] To borrow freely from the conclusions of Kathryn Sikkink latest book "The Justice Cascade" where she investigates the development of one particular norm, that of individual criminal responsibility for human rights violations. Kathryn Sikkink, **The Justice Cascade: How Human Rights Prosecutions Are Changing World Politics,** W. W. Norton, 2012

[5] Daniel Bethlehem, *The End of Geography: The Changing Nature of the International System and the Challenge to International Law*, **The European Journal of International Law** *Vol. 25 no. 1, 2014.*

[6] To borrow from Bethlehem but others have used this as well.

[7] T*he individual*, thanks to technology, is abled and free to take a more active economic and political role

[8] Yochai Benchkler, **The wealth of Networks: how social production transforms Markets and Freedoms**, Yale University Press, 2006; Manuel Castells

[9] Milton Mueller, **Networks and States, the Global Politics of Internet Governance**, London: MIT Press, 2011 - Ebook version, (location 86)

[10] "Much of Internet governance is enacted by private corporations and non governmental entities" - Delegated censorship, delegated surveillance, delegated copyright enforcement, and delegated law enforcement have shifted governance – for better or for worse – to private intermediaries… (p.11, de Nardis)

[11] Tim Wu, **the Master Switch**, New York: Knopf, 2010

conceptions of international society and of international law[12], producing, what Milton Mueller so rightly refers to as, "institutional innovation in the global regulation of information and communication"[13].

Yet, the State cannot and could not be ignored. The conviction that the Internet and its digital communities were establishing a new mode of global governance, with its own inherent global values, was shattered in the summer of 2013. Edward Snowden's revelation of massive NSA surveillance of Internet transactions points to the return, in force, of the State - seeking to assert control over what had been thought as the "ungovernable" Internet. However, the centrality of the State to Internet governance is not quite as new as some observers may believe. Already in 2006, the historical transformation of Internet governance towards greater State control was well captured by Lessing when he wrote:

> *"The first generation of these architectures was built by a noncommercial sector—researchers and hackers, focused upon building a network. The second generation has been built by commerce. And the third, not yet off the drawing board, could well be the product of government. Which regulator do we prefer? Which regulators should be controlled? How does society exercise that control over entities that aim to control it?"*[14]

As a human rights activist working in the field of freedom of information and expression over the last 10 years, my experience has been indeed that of a constant battle against the over-reach of the State into the soul of the technology and against the rights of its users, with the result that millions are *"either access poor, access denied or access repressed*[15].

The role of the State over Internet regulation and on-line content is powerful and well established, with the Chinese Firewall by no means the only example. It may suffice here to point to some of the facts indicating the current pre-eminence of the State in cyber space:

- The explosion of laws and decrees by governments and parliaments is not a development of the last year but one that can be traced back over the past decade or more[16]. The momentum behind the governmental search for regulation, control and standards of behaviours on-line can be partly explained by cybercrime (e.g. theft identity, card fraud, email hacking, physing and spam) and on-line illegal content (e.g. child pornography) – most of which may be considered to be legitimate areas for state interventions. But laws targeting legitimate on-line expression and content have also multiplied, including those related to intermediaries' liability for copyright infringements. Many have increased the penalties and lowered the threshold for illegitimate on-line speech in relation to alleged offensiveness, national security, etc.[17] Arbitrary blocking and filtering of content, along with the criminalisation of legitimate

[12] Bethlehem, p.18
[13] Mueller, Networks and States, Kindle version, location 29
[14] Lawrence Lessig, Code version 2.0, 2006, p.22
[15] Agnes Callamard, "Keynote Speech", in ASEM, Human Rights and Information and Communication Technology, Proceedings of the 12th Informal Asia-Europe Meeting (ASEM) Seminar on Human Rights, Asia-Europe Foundation, 2013, p.10 http://www.asef.org/images/stories/publications/documents/ASEF-12th_HR_Seminar_Publication.pdf
[16] Over the last decade, governments have enacted laws and regulations addressing online speech, most of which have been regressive in nature and have imposed restrictions that do not meet the legitimacy conditions set out in international human rights standards. See UNESCO, World trends in freedom of expression and media development, 2013, p.32. http://unesdoc.unesco.org/images/0022/002270/227025e.pdf#page=26
[17] International human rights standard and international jurisprudence concur in their finding: offensive speech should be protected, be they on or off line. See Human Rights Committee, General Comment 34, 2011. http://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf

expression on-line, have been highlighted as major areas of concern for close to 10 years, and certainly over the last five[18].

- In 2007 already, the Committee to Protect Journalists (CPJ) referred to the imprisonment of journalists as a **continuing decade-long trend**[19]. In 2008, CPJ had found that "more Internet journalists are jailed worldwide today than journalists working in any other medium… 45 percent of all media workers jailed worldwide are bloggers, Web-based reporters, or online editors"[20]. In 2014, it was 54% of all journalists imprisoned for "speech crimes" that were working on-line.[21]
- The intrusion of the State into the Internet world has steadily increased. In its latest Internet Freedom report, Freedom House reports that 34 out of the 60 countries assessed experienced a negative trajectory during the coverage period. The report goes on to identify "*the proliferation of laws, regulations, and directives to restrict online speech; a dramatic increase in arrests of individuals for something they posted online; legal cases and intimidation against social-media users; and a rise in surveillance*". These, Freedom House asserts, are the key drivers behind the overall decline in Internet freedom in the past year.[22]
- Another indicator of the importance of the nation-state and geography in digital governance is the multiplication of policies and regulations enacted by the expert branches of government at national, regional and, increasingly, the international levels, as particularly well demonstrated by the regulatory policies of the European Union and the US government and the (secret) negotiations over a range of trade agreements, such as the Trans-Pacific Partnership.

The Courts have not been absent from these developments. In addition to their contribution to the high rate of imprisonment for on-line content, courts have been asked, amongst other things, to address the thorny issue of whether and how far does national jurisdiction apply to global Internet. For instance, as early as 2000, territorial sovereignty was asserted in France resulting in the US company Yahoo having to ensure that French residents could not access content on a site that violated French law, in this case through posting of Nazi memorabilia[23]. It was again asserted 14 years later in when the European Court of Justice ruled that the operator of a search engine must be considered to be a "data controller" and that the Google Spain "establishment" in Spain includes processing personal data "in the context of its activities"[24]. Indeed, the assertion of national jurisdictions over a US company and/or a global technology is increasingly becoming the norm rather than the exception[25].

Overall though, tribunals have been seen as a marginal player as far as Internet regulation is concerned. Technological developers/innovators, Internet users themselves, the corporate sector, politicians and "experts", including at governmental and civil society levels, have played a far greater role in terms of regulating Internet, on-line content and freedom of expression on-line. These actors, alone or in combination, have been particularly at the

[18] See for instance the 2011 report by the UN Special Rapporteur on freedom of expression focusing on Internet http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[19] CPJ, 2007 Prison Census: https://cpj.org/reports/2007/12/journalists-in-prison-in-2007.php
[20] CPJ, 2008 Prison Census, https://www.cpj.org/reports/2008/12/cpjs-2008-prison-census-online-and-in-jail.php
[21] Committee to Protect Journalists, https://cpj.org/imprisoned/2014.php
[22] Sanja Kelly, "Despite pushbacks, Internet Freedom deteriorates" in Freedom House, Freedom on the Net,
[23] LICRA vs. Yahoo, May 2000
[24] http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=en
[25] http://www.internetjurisdiction.net This trend is very clear as far as copyright is concerned, with governments, beginning with the US, seeking to impose copyright obligations extra-territorially.

forefront of developing the **norms** for the Internet revolution. Tribunals have had difficulties both in terms of understanding these values or norms[26], or influencing them.

A quick word about norms development

It is beyond the purpose of this paper to offer a comprehensive review of the literature on norms development. I will here quickly identify some of the key features of the norms development process as identified by two lead thinkers in the field, Finnemore and Sikkink.[27] Finnemore and Sikkink define norms as a "*standard of appropriate behavior for actors with a given identity*", and distinguish this definition and approach from that of institutions, which suggest a "*collection of practices and rules*". They argue that norms go through a life cycle composed of three phases: norm emergence, norm cascade and norm internalization, the first of which relies heavily on a norm entrepreneur. Norms entrepreneurs arise (randomly) *with a conviction that something must be changed*, using existing organizations and norms as a platform from which to proselytize, *framing their issue* to reach a broader audience.

> *"The characteristic persuasion of the first stage, norm emergence, is persuasion by norm entrepreneurs. Norm entrepreneurs attempt to convince a critical mass of states (norm leaders) to embrace new norms. The second state is characterized more by a dynamic of imitation as the norm leaders attempt to socialize other states to become norm followers… A combination of pressure for conformity, desire to enhance international legitimation, and the desire of state leaders to enhance their self-esteem facilitate norm cascade. At the far end of norm cascade norm internalization occurs: norm acquire a taken for granted quality and are no longer a matter of broad public debates[28]."*

In stage 2, states adopt norms in response to international pressure--even if there is no domestic coalition pressing for adoption of the norm. "*They do this to enhance domestic legitimacy, conformity, and esteem needs [because being shamed as non-conformists by the int'l community makes them feel bad]"*. In the last stage, norm internalization, "*we internalize these norms. Professionals press for codification and universal adherence. Eventually, conformity becomes so natural that we cease to even notice the presence of a norm.*"

Finnemore and Sikkink warn us though that completion of the life cycle is not an inevitable process and that a number of norms may never get to the tipping point allowing for norms cascade and norms internalization. This unstable state of affairs may be particularly true as far as Internet is concerned. The norms development process in this global cyberspace is particularly complicated in that it concerns not only States behaviors but many others, equally important, including individual users (an arguably very disparate group), Engineers/Programmers, the Corporate Sector (including the very vast categorie of Intermediaries) and a number of historically-imposed institutions (eg ICANN).

A recent conference in Sao Paulo attempted to bring all these actors together (the so-called multi-stakeholder approach) to define, if not somehow codify, the norms that should govern the governance and regulation of cyberspace. The NetMundial outcome document, adopted by "rough consensus" comes as close as can be to constitute (in theory) *the* global

[26] One often-heard comment from cyber activists, NGOs and lawyers is that Judges simply do not understand the technology. They belong to a different generation (understand older), and were not trained in the emerging and rapidly changing technological law.

[27] Martha Finnemore and Kathryn Sikkink , International Norms Dynamics and Political Change in *International Organization, Vol.52, No.4, 1998: pp.887-917.* See also Kathryn Sikkink, Transnational Politics, International Relations Theory, and Human Rights, in *Political Science and Politics*, Vol. 31, No. 3, (Sep., 1998), pp. 516-523

[28] Finnemore and Sikkhin, 1998, op.cit., p.895

normative framework for cyberspace. It identifies key governance principles, including freedom of expression and information and the right to privacy, and limited intermediary liability. It reiterates that *"Internet should continue to be a globally coherent, interconnected, stable, unfragmented, scalable and accessible network-of-networks, based on a common set of unique identifiers and that allows data packets/information to flow freely end- to-end regardless of the lawful content*[29]*."* All stakeholders involved in the governance of Internet should seek to achieve "*security, stability and resilience of the Internet*". They should collaborate, preserve innovation and openness. The norms of behaviour were drafted in general enough terms to generate "rough" consensus at the time and ultimately a sense of achievement amongst many involved, whether States, corporations, or NGOs[30]. And yet, within the same year the document was adopted, governments continued to issue specific laws and policies regulating and limiting on-line content; divergences over the global governance of Internet continued unabated[31], and legal conflicts (at domestic level) over a range of on-line issues (intermediary liability, copyright, hate speech, etc.) multiplied[32]. All of these demonstrate conflicts over the norms that should govern the Internet world, and indeed a possible recrudescence of these conflicts, with tribunals and Judges adding to the normative uncertainty (as counter intuitive as this may stand).

II - 2014: a watershed for judicial regulation?

Recent judicial decisions may well have been a watershed as far as the judicial regulation of social platforms and "intermediaries" are concerned. Time will tell whether these are long standing trends or accidental ones.

2014 stands out not because of court-ordered "dragnet" blocking of an entire platform, or more targeted blocking of specific websites or pages[33], an "old" phenomena and extreme forms of regulation, which says as much about judicial independence as it does of Internet regulation. Rather, 2014 stands out because it demonstrates the emergence of a judicial expertise *and confidence* in reviewing and challenging technological-based assumptions and, to a large extent and by implication, technologically-derived norms[34].

II.1 A News Portal as a Publisher Liable For Its Readers' Comments

The European Court for Human Rights determined that a (mostly) user-generated news portal is in fact a *publisher* and thus liable for the comments of its readers.

In ***Delfi v Estonia***[35]*,* the European Court for Human Rights held that Delfi (one of the largest Internet portals in Estonia) "was *in a position to know about an article to be published, to*

[29] NetMundial Outcome Document: http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

[30] The process and outcome were decried though by China, Russia, Saudi Arabia, and to a lesser extent, India.

[31] Two conflicts have dominated the agenda in recent years: that between the US and China and the conflicts over the scope of NSA surveillance with Brazil and Germany playing a key role in challenging the US and the 5 Eyes practices.

[32] To these should be added the older conflict over extra-territorial obligations and the newer one over surveillance. See Agnes Callamard, Global trends in freedom of expression jurisprudence in 2014, Global Freedom of Expression @Columbia, 2014

[33] However, remarkable rulings by the Turkish Constitutional Court on these questions also stand out and may become a reference for media lawyers and activists alike in the years to come – and hopefully for courts as well.

[34] Of course, not all of 2014's decisions related to Internet and freedom on-line established new ground with large policy and behavioural implications. Some built on existing jurisprudence and precedent, e.g. as far as intermediary liability or right to privacy are concerned. Further, it is possible that some of the 2014 decisions will be overturned in 2015 or later on.

[35] http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-126635#{"itemid":["001-126635"]}

predict the nature of the possible comments prompted by it and, above all, to take technical or manual measures to prevent defamatory statements from being made public". Many observers and free speech activists, along with users of social media, have lamented the ruling and the implications it holds for the liability of "intermediaries".

The decision makes multiple references to Delfi acting as a publisher, as opposed to being a "neutral" service provider whose conduct can be deemed to be merely technical, automatic and passive (as per the distinction drawn by *Google France* and *Google* [2010] ECR I−2417).

The Court fails to thoroughly back up its definition of what Delfi constitutes: in its decision's paragraph 50, reviewing the admissibility of the case, the Court:

> "*notes that the applicant company was sued for defamation in respect of comments posted on its Internet portal, it was deemed to be discloser (or publisher – the Estonian words avaldama/avaldaja mean both disclose/discloser and publish/publisher; see, for example, paragraphs 36 and 38 above) of the comments – along with their authors – and held liable for its failure to prevent the disclosure of or remove on its own initiative the unlawful comments*."

The Court provides additional explanation in Paragraph 75, linking its determination of Defli as a publisher to the application of existing tort law:

> *The fact that in the present case publication of articles and comments on an Internet portal was also found to amount to journalistic activity and the administrator of the portal as an entrepreneur was deemed to be a publisher can be seen, in the Court's view, as application of the existing tort law to a novel area related to new technologies (compare, for example, Bernh Larsen Holding AS and Others v. Norway, no. 24117/08, § 126, 14 March 2013, where the Court saw no reason to question the domestic court's interpretation, according to which legal provisions originally conceived in respect of hard copies of documents were also deemed to apply to electronically stored documents).*

Throughout its review of the merits of the case, the Court insists on describing Delfi as a professional publisher (e.g. in par. 76.), a media publisher or more generally a publisher. In essence, the Court held Delfi to constitute a primary publisher, exercising direct editorial control over the published statements.

Once this was established, and given the fact that there was no dispute that the comments posted by readers in response to a news article were actually libelous, the conclusion that Delfi was liable for the comments was almost self-evident. The Court did review the mechanisms Delfi had put in place to respond to libelous, obscene or violent comments, including an automatic deletion based on some key words, and a notice and take down system – both of which were judged insufficient for its exercise of due diligence (as a publisher). It ultimately concluded that based on:

> *"…the insulting and threatening nature of the comments, the fact that the comments were posted in reaction to an article published by the applicant company in <u>its professionally-managed news portal</u> run on a <u>commercial basis</u>, the <u>insufficiency of the measures</u> taken by the applicant company to avoid damage being caused to other parties' reputations and to ensure a realistic possibility that the authors of the comments will be held liable, and the moderate sanction imposed on the applicant company, the Court considers that in the present case the domestic courts' finding that the applicant company was liable for the defamatory comments posted by readers on its Internet news portal was a justified and proportionate restriction on the applicant company's right to freedom of expression. There has accordingly been no violation of Article 10 of the Convention."*

The Delfi decision challenged existing notions in several ways:

- It imposes a different definition of a web platform – away from that of a "simple" technical intermediary, towards that of a publisher
- It determines that as such, the owner is liable for third party comment made on its website
- It insists that Delfi mechanisms to address libelous content were insufficient, including its *notice* and *take-down* system and thus suggested that Delfi should *prevent* defamatory and other 'clearly unlawful' comments from being made public (e.g. by moderating comments).

Press freedom organizations and international media and Internet companies have lamented the decision, and warned against its "*serious adverse repercussions for freedom of expression and democratic openness in the digital era. In terms of Article 43 (2) of the Convention, we believe that liability for user-generated content on the Internet constitutes both a serious question affecting the interpretation or application of Article 10 of the Convention in the online environment and a serious issue of general importance."*[36]

In a subsequent case in Ireland[37], the judge considered the application of the Delfi logic to Facebook but rejected it. *"On the evidence open to me at the moment, it does seem that monitoring all the possible websites could impose a disproportionate burden on the defendant. Of course the plaintiffs will be able to seek further relief from this court if there is any recurrence of the offending publications. It will then be open to Facebook, acting responsibility and in accordance with their principles, to proactively take the steps for necessary removal and closure."* The Judge concluded by suggesting *"Time will tell whether the line of reasoning of the ECHR in this case is the start of a new movement towards a broader monitoring obligation of intermediaries or if it is only applicable to the specific events in this case."*[38]

On the other hand, it is clear that the ECfHR judges ultimately agreed with the Estonian government view that Delfi is no Facebook. The decision matters not only because of the liability implications but as importantly because of the rationale for it: not all intermediaries are the same.

The Delfi decision may prefigure a more segmented and diverse legal understanding of "intermediary," one which will recognize the multiplicity of their forms, mandates, control of and interaction with content[39].

---

[36] 69 media organisations, internet companies, human rights groups and academic institutions write to support the referral request that we understand has been submitted in the case of *Delfi v. Estonia* (Application No. 64569/09) http://www.article19.org/data/files/DelfiGCreferral_letterinsuppt_clean_20140113-1.pdf

[37] J19 & Anor v Facebook Ireland [2013] NIQB 113 (15 November 2013)

[38] http://www.bailii.org/nie/cases/NIHC/QB/2013/113.html

[39] In a 2013 European case regarding the Google blogger platform, this later was held to be neither a primary nor a secondary publisher pre-notification, but a publisher **post-notification**. Under **Tamiz V Google,** 19 March 2013, the UK Court of Appeal was asked to determine whether Goggle was liable for defamatory comments posted to a blog hosted on its blogger platform. The Court of Appeal held that *"If Google Inc. allows defamatory material to remain on a Blogger blog after it has been notified of the presence of that material, it might be inferred to have associated itself with, or to have made itself responsible for, the continued presence of that material on the blog and thereby to have become a publisher of the material."* The Court of Appeal said that no inference of publication should be drawn until Google had had a reasonable time in which to act to remove the defamatory comments; and that it was arguable that five weeks was sufficiently long for an adverse inference to be drawn against Google. Reference [2013] EWCA Civ 68. Court of Appeal. Judge Master of the Rolls, Richards LJ, Sullivan LJ. Date of Judgment 14 Feb 201. The judgment may be found here:

The Delfi decision has been referred to the Grand Chamber of the Court for reconsideration in 2014 but no ruling has been rendered at the time of writing this analysis.

II.2. Search Engines as Controller of Data

In its ruling of 13 May 2014, in ***Google Spain SL, Google Inc. v Agencia Española de Protección de Datos, Mario Costeja González*** **(2014)**[40]**,** the so-called "Right to be Forgotten" case, the European Court of Justice applied a European Directive on data protection[41] to establish the following precedents:

The Court first determined that a **Search Engine** collects**,** retrieves, organizes, stores and discloses information – all of which actions amount, altogether, to **processing data:**

> "*Therefore, it must be found that, in exploring the Internet automatically, constantly and systematically in search of the information which is published there, the operator of a search engine 'collects' such data which it subsequently 'retrieves', 'records' and 'organises' within the framework of its indexing programmes, 'stores' on its servers and, as the case may be, 'discloses' and 'makes available' to its users in the form of lists of search results. As those operations are referred to expressly and unconditionally in Article 2(b) of Directive 95/46, they must be classified as 'processing' within the meaning of that provision, regardless of the fact that the operator of the search engine also carries out the same operations in respect of other types of information and does not distinguish between the latter and the personal data."[ar.28]*

The Court further determined that a Search engine is the **controller** of the data it has processed:

> *"It is the search engine operator which determines the purposes and means of that activity and thus of the processing of personal data that it itself carries out within the framework of that activity and which must, consequently, be regarded as the 'controller' in respect of that processing" [Par.33]*

The Court then rejected the argument that the processing of personal data by Google Search is not carried out by Google Spain (meaning by Google *in Spain*) but is carried out by Google Inc., which operates Google Search without any intervention by Google Spain. The Court argued that the processing of personal data is carried out "**in the context of the activities**" of Google Spain:

> *"the very display of personal data on a search results page constitutes processing of such data. Since that display of results is accompanied, on the same page, by the display of advertising linked to the search terms, it is clear that the processing of personal data in question is carried out in the context of the commercial and advertising activity of the controller's establishment on the territory of a Member State, in this instance Spanish territory." [Par. 57]*

---

http://www.bailii.org/ew/cases/EWCA/Civ/2013/68.html Analyses and comments include: http://cyberleagle.blogspot.com/2013/03/tamiz-v-google-court-of-appeal-verdict.html; http://www.scl.org/site.aspx?i=ed31376

[40] http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=DOC&docid=152065&occ=first&dir=&cid=667631

[41] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The Court went on to determine the scope of the *right to be forgotten* and how it should thus be implemented:

> *"If the data appear to be inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they were processed, the information and links concerned in the list of results must be erased."* [Par. 93 and 94].

The Court recognizes freedom of the press in Paragraph 85, when it rules that the data subject may be capable of exercising his right (to be forgotten) against a Search Engine but **not against the publisher of a webpage**.

The Court also acknowledges a different treatment in case of data concerning an individual in the public eye, justifying a preponderant interest of the public in having access to the information when such a search is made. But overall, the judgment is clearly placing a heavier focus on the protection of the right to privacy:

> *"As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the information in question no longer be made available to the general public by its inclusion in such a list of results, it should be held, as follows in particular from paragraph 81 of the present judgment, that those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name."*

The right to be forgotten and the ECJ ruling were invoked almost immediately across and outside Europe, in the UK, France, Israel, the Netherlands[42], Canada[43], Mexico. Some of those decisions further detailed and extended the reach of the original ECJ decision.

The decision of the **Supreme Court of British Columbia** signaled that the "right to be de-linked" could be invoked and implemented world-wide, thus extending potentially the geographical scope of the original decision. The Supreme Court issued an order requiring Google to remove websites from its **worldwide index** in Equustek Solutions Inc. v. Jack. The Court of Appeal subsequently accepted Google appeal but did not grant the stay, so the injunction remains in place.

The **Dutch court judgment**[44] was important in that it elaborated further on the decision of the European Court of Justice and in so doing, reached a stronger balance between the protection of the right to privacy and that of freedom of expression and information.

Joran Spauwen and Jens van den Brink, analysing the Dutch court decision, point out that it gave a "personal twist" to the test provided by the CJEU:

> *"The [Google Spain] judgment does not intend to protect individuals against all negative communications on the Internet, but only against 'being pursued' for a long time by 'irrelevant', 'excessive' or 'unnecessarily defamatory' expressions*,"

Quoting from the Dutch ruling, Spauwen and van den Brink note that:

> *"The elements 'being pursued for a long time' and 'unnecessarily defamatory' are not quotes from Google Spain. Apparently the Dutch Court read those elements in the CJEU decision. The interpretation by the Dutch court provides a more balanced view than that of the Luxembourg Court, because it does not imply that privacy*

[42] C/13/569654 / KG ZA 14-960, 19-09-2014, Rechtbank Amsterdam

[43] *Equustek Solutions Inc. v. Jack*, 2014 BCSC 1063 (CanLII) http://www.courts.gov.bc.ca/jdb-txt/SC/14/10/2014BCSC1063.htm

[44] http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118

outweighs free speech and the freedom of information (which the CJEU literally considered in the Google Spain decision).[45]"

Consequences

Much has been written on the impact of the ruling on the Internet, Google and freedom of expression[46]. Google reported that, as of November 2014, it had received 166,396 requests for URL removals[47]. Facebook is the website that has had the most requests for URL removals (with 3797 removed as at 13 November 2014), followed by profileengine.com (with 3707 removals)[48]. Out-of-court settlements between Google and "data subjects" seeking the removals of search links may become the norm.[49] Crucially, there is increasing pressure, including legal pressure, to interpret the CJEU ruling as having a global reach, not just limited to European countries[50].

What has not been so well highlighted thus far is that, for some years now, grass root social movements in Europe have called for a right to be forgotten, alarmed by the lasting consequences of on-line posting. Hence, in France, for instance, in 2010 as a result of pressures emanating from associations of parents, as well as children rights and catholic organisations, the Government adopted two charters related to the right to be forgotten[51]. [52]. To a large extent, the ECJ decision was in fact very much in keeping with a strong social demand, at least in Europe, regarding privacy in general.

This is not just a European or Spanish or French movement. In September 2013, California passed the so-called California Eraser Statute, requiring:

---

[45] Dutch Google Spain ruling: More Freedom of Speech, Less Right To Be Forgotten For Criminals http://inforrm.wordpress.com/2014/09/27/dutch-google-spain-ruling-more-freedom-of-speech-less-right-to-be-forgotten-for-criminals-joran-spauwen-and-jens-van-den-brink/#more-27910

[46] See for instance the various analyses on Inforrm's blog: http://inforrm.wordpress.com/?s=right+to+be+forgotten

[47] Google, Transparency Report: European privacy requests for search removals, November 2013 http://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

[48] For an analysis of the removal, see Sara Mansoori and Eloise Le Santo, "Over half a million Google URLs removal requests to date; the "Right to be Forgotten" in practice ", Inforrm's Blog, November 2014 http://inforrm.wordpress.com/2014/11/14/over-half-a-million-google-urls-removal-requests-to-date-the-right-to-be-forgotten-in-practice-sara-mansoori-and-eloise-le-santo/#more-28462

[49] The Guardian reported that Google appears to have agreed to increase its efforts to remove online links to malicious articles that made false allegations about an international businessman. Settlement of what would have been a test case defining the US firm's global responsibilities was reached in the case brought by the former Morgan Stanley banker Daniel Hegglin against the search engine company after allegations were circulated across 4,000 websites in what was described by his lawyers as an extreme example of internet trolling. Details of the settlement were not revealed but an agreed statement was read out in court. "The settlement includes significant efforts on Google's part to remove the abusive material from Google-hosted websites and from its search results," said Hegglin's barrister, Hugh Tomlinson QC. http://www.theguardian.com/technology/2014/nov/24/google-settles-online-abuse-court-case-daniel-hegglin

[50] See for instance the global injunction against Google provided by the Supreme Court of British Columbia in Canada, in *Equustek Solutions Inc. v. Jack*.

[51] See for instance: "Droit à l'oubli" sur Internet : une charte signée sans Google ni Facebook", Le Monde, 13 November 2010, http://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html See also, Le Petit Juriste, Internet et le droit à l'oubli numérique, 23 February 2011, http://www.lepetitjuriste.fr/divers/internet-et-le-droit-a-loubli-numerique

[52] See for instance: "Droit à l'oubli" sur Internet : une charte signée sans Google ni Facebook", Le Monde, 13 November 2010, http://www.lemonde.fr/technologies/article/2010/10/13/droit-a-l-oubli-sur-internet-une-charte-signee-sans-google-ni-facebook_1425667_651865.html See also, Le Petit Juriste, Internet et le droit à l'oubli numérique, 23 February 2011, http://www.lepetitjuriste.fr/divers/internet-et-le-droit-a-loubli-numerique

> *"the operator of an Internet Web site, online service, online application, or mobile application to permit a minor who is a registered user of the operator's Internet Web site, online service, online application, or mobile application, to remove, or to request and obtain removal of, content or information posted"*[53].

While far narrower in terms of the scope and the audience concerned than the ECJ right to be delinked decision, the California eraser statute underscores social anxieties and pressures, and the determination of the political and legislative sectors to draw on the law to establish some boundaries. A number of other legal initiatives to address and curtail "*revenge porn*[54]," and "*mug shot websites*[55]" testify to the increasing conflicts over the reach and use of Internet.

II.3. Search Engine as an Editor

In Zhang v Baidu[56], a New York judge rejected as well the notion of search engines as mere technical conduit to rule that a search engine's editorial function is much like the editorial function of other media publishers. The implication of this characterization stands in sharp contrast with that on the right to be de-indexed. Because search engines results are the productf ditorial choices, they are protected by the First Amendment against government interventions.

The case concerned the Chinese language search engine Baidu's operations in the United States. A New York based Non-Governmental Organisation sued Baidu for conspiring to prevent "pro-democracy political speech" from appearing in its search-engine results in the U.S., alleging that Baidu omitted their work at the behest of Chinese government. Baidu argued (ironically) that its search algorithm was an expression of its own views, values and opinions and, as such, was protected speech under the First Amendment. The Judge agreed[57].

He first determined that:

> *"The central purpose of a search engine is to retrieve relevant information from the vast universe of data on the Internet and to organize it in a way that would be most helpful to the searcher. In doing so, search engines inevitably make editorial judgments about what information (or kinds of information) to include in the results and how and where to display that information (for example, on the first page of the search results or later)… In these respects, a "search engine's editorial judgment is much like many other familiar editorial judgments," such as the newspaper editor's judgment of which wire-service stories to run and where to place them in the newspaper, etc."*

He then goes on to reject a series of alternative proposals or elements that could influence the first amendment protection:

(i) The possible distinction between opinions and facts:

> *"[t]he fact that search-engines often collect and communicate facts, as opposed to*

---

[53] http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568

[54] For a balanced free speech analysis, see: http://www.article19.org/join-the-debate.php/168/view/

[55] See a short overview here: http://www.nolo.com/legal-encyclopedia/are-mug-shot-websites-legal.html

[56] The judgment may be found here: http://blogs.reuters.com/alison-frankel/files/2014/03/zhangvbaidu-opinion.pdf

[57] See analysis by Monica Goyal, **Freedom of speech gives Baidu right to censorship, judge rules,** April 15, 2014, in **itbusiness.ca** http://www.itbusiness.ca/blog/freedom-of-speech-gives-baidu-right-to-censorship-judge-rules/48052

opinions, does not alter the analysis. As the Supreme Court has held, "the creation and dissemination of information are speech within the meaning of the First Amendment. Facts, after all, are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs."

(ii) The fact that search-engine results may be produced algorithmically:

"After all, the algorithms themselves were written by human beings, and they "inherently incorporate the search engine company engineers' judgments about what material users are most likely to find responsive to their queries."

(iii) The idea that search engines, as mere technical conduits, are deserving of a lower protection under the first amendment, similar to the protected afforded to cable companies.

"it is debatable whether any search engine is a mere "conduit" given the judgments involved in designing algorithms to choose, rank, and sort search results... But whether or not that proposition is true as a general matter, it is plainly "not apt here," as Plaintiffs' own allegations of censorship make clear that Baidu is "'more than a passive receptacle or conduit for news, comment, and advertising.'"

And the Judge to conclude that *"Accordingly, to allow Plaintiffs' suit to proceed, let alone to hold Baidu liable for its editorial judgments, would contravene the principle upon which "[o]ur political system and cultural life rest": "that each person should decide for himself or herself the ideas and beliefs deserving of expression, consideration, and adherence."*

A few months later, in California, in **St. Louis Martin v. Google,** a Judge granted Google's motion to apply California's "anti-SLAPP" law, which allows a court to efficiently dismiss lawsuits against acts protected as free speech. The Court ruled in essence that Google search results were protected by the First Amendment ("constitutionally protected activity"), and that the plaintiff failed to produce any evidence "supporting a probability of success"[58].

The US and European positions have not necessarily grown further apart in 2014. In fact, the 2014 judgments on both side of the Atlantic recognize that Search Engines have control over the data they collect, although the US position goes so far as to describe such functions as amounting to those of *publishing* and *media*. Under neither jurisdiction are Search Engines or the algorithms behind them considered to be only neutral technology[59].

Where the Courts disagree is on the implications of the (editorial or publishing) control that they ascribe to Search Engines. In Europe, this control is understood to mean that Search Engines are liable for their search results (i.e. links to websites), and may have to erase such links (in application of the right to be forgotten). In the US, this control protects Search Engine from such liability (except, of course, in cases allowed for under the first amendment).

The Argentinean Supreme Court offered a third route and accompanying reasoning in 2014 in its October ruling of ***Belén Rodriguez v. Google***. The case focused initially on the question of whether search engines are strictly liable for unlawful third-party content appearing in search results. The court unanimously dismissed claims that the defendants had engaged in inherently risky activities and should therefore be subject to no-fault liability for harm to third parties (on the basis that Search Engines cannot be expected to police the content of their search results). The Court further insists, in keeping with precedents, that ***Search***

[58] http://cdn.arstechnica.net/wp-content/uploads/2014/11/Order.pdf

[59] There are exceptions to this conclusion, particularly in situations concerning copyright infringements that I am not considering in this analysis.

Engines are only liable if they have effective knowledge *of a third-party violation and do not take the steps necessary to prevent further damage.*

However, the Court goes on to identify two mechanisms of notification. The first, offering the greater guarantee for freedom of expression **is the notification by a judicial authority of the illegality of a third-party content. The second mechanism is notice by the affected party** in cases that involve content which illegality is clear and beyond any possible doubt and causes "gross and manifest harm[60]". As subsequent analysts have pointed out, these exceptions though are somewhat broad and open to interpretation. They include child pornography and unlawful publication that "grossly violate" individuals' privacy, revelations of secret judicial investigations, hate speech, etc. *"Some of the examples provided by the Supreme Court as exceptions to the judicial notice concern speech that is protected by our laws and by Argentina's Supreme Court precedents[61]."*

II.4. Google Autocomplete As A Publisher

The Google autocomplete function was not the subject of much debate in 2014 (with a notable exception discussed below) but it has emerged as a new area of law, which will no doubt deliver a range of interesting perspectives in the years to come.

In 2013, a German federal court had ordered Google to remove offensive or defamatory search suggestions when it was notified of an unlawful violation of a person's rights, rejecting Google's argument that its automated process merely reflected the search words used by other people, and could not be modified.

In 2014, in Hong Kong, entertainment tycoon Albert Yeung Sau-shing brought a law-suit against Google, because the "autocomplete" function of its search engine linked him to triad gangs[62].

A Court of First Instance in Hong Kong determined that "whilst the algorithms use several factors outside of Google's control, it is:

> "*arguable that Google Search does not simply convey information, but its Autocomplete and Related Searches features act by providing information distilled pursuant to artificial intelligence set up by Google Inc themselves by virtue of the algorithms they have created and maintained to actively facilitate the search processes*."

The Court also argued that the evidence demonstrated that Google was capable of censoring material generated through its searches. Accordingly, it was questionable whether Google is a "neutral tool" and therefore there was "*a good arguable case that Google Inc. is more than a passive facilitator vis-à-vis their Autocomplete and Related Searches features"*[63].

In October, Google was given permission to appeal against the ruling that Hong Kong had jurisdiction to hear the defamation lawsuit.

---

[60] Entremedios, **Internet Service Providers liability in Argentina: Rodriguez vs. Google,** 18 December 2014 http://entremedios.org/2014/12/18/internet-service-providers-liability-in-argentina-rodriguez-vs-google/

[61] Entremedios, op.cit.

[62] Albert Yeung Sau-shing wants a court to order Google to remove the defamatory suggestions and to compensate him. http://www.scmp.com/news/hong-kong/article/1627777/google-appeal-against-jurisdiction-tycoons-lawsuit

[63] Herbert Smith Freehills LLP, Gareth Thomas and Dominic Geiser, Hong Kong Court of First Instance allows Albert Yeung's libel case in relation to Google's autocomplete search function to proceed, in Lexology, 19 August 2014, http://www.lexology.com/library/detail.aspx?g=6a556fa8-7989-4fda-b6c1-ed246d5c0c47

In Conclusion

Throughout 2014, courts around the world have asserted their national (or regional) jurisdiction over Internet (its content, users and actors), the global (American mostly) companies that manage it[64] and the working of the technology itself.

For the purpose of this discussion paper, the definition of norms was borrowed from Finnemore and Sikkink to mean "*standard of appropriate behavior for actors with a given identity.*" The decisions highlighted above have large implications for the ways "intermediaries" behaved but also users and governments. A few conclusions may be highlighted with regard to norms development and conflict.

First, the rulings stand out because they were directly related to the technology or the algorithm – the *medium* through which the speech is communicated - rather than (solely) the *content* of the speech. They rejected the idea of a "neutral technology", or that of a technology driven by its own inherent logic that cannot be altered. In effect, the decisions sought to "reign in" technology and the institutions that own, manage or develop it.

Second, the rulings challenged the end-to-end principle and the dominant paradigm as far as Intermediaries are concerned. The "right to be delinked" decision introduces a number of human interventions that weaken the global and technical "coherence" of Internet. The rulings related to the search engines recognise the independent editorial role of some intermediary in their management of, and influence over, search results.

Thirdly, the decisions introduced legal variety in the concept of "intermediaries" with large implications for their standards of behaviours particularly related to content monitoring and moderation. This stands in possible contradiction with NetMundial outcome document, which states, amongst its key Internet principles, that *"Intermediary liability limitations should be implemented in a way that respects and promotes economic growth, innovation, creativity and free flow of information. In this regard, cooperation among all stakeholders should be encouraged to address and deter illegal activity, consistent with fair process."* The decisions also have potential implications for the nature and dynamics of freedom of expression on-line, bringing it one step closer to traditional (read hierarchical and regulated) relationships between the creators and users of news.

Fourthly, the decisions reflect societal concerns and anxieties over the Internet, but they also channel the demands "for a say" over its governance and regulation by those that were not part of the first or second generation of Internet actors.

The norms development and cascade processes highlighted previously are made particularly complex because of the Internet's own success: "new" actors emerge constantly, shaping the Internet world and influencing the development of norms, values, behaviours. Some had been left initially at cyberspace margins - because of their geographical location (the infamous "digital divide") or lack of technical know-how or because they had been too slow in picking up on the political, economic or social significance of Internet. Others are part of a new digital generation.

The originally "not-in-the-loop" groups and individuals (from politicians to legislators to parents) and an increasing number of digitally fluent actors and users, are all asserting and claiming a role and a voice in the running of the digital world; one that leads them to question the norms (including principles and/or behaviors) developed by the initial digital

[64] http://www.internetjurisdiction.net This trend is very clear as far as copyright is concerned, with governments, beginning with the US, seeking to impose copyright obligations extra-territorially.

generations or indeed, by the corporations that are dominating its working. And so the associated social and legal norms are advanced, tested and contested, with a range of actors finding, strengthening or shifting their places in the Internet chess game, scripting their roles and deciding on their next moves.

This makes for a fantastically complex environment – one which theorists of norms development may not have quite foreseen.

The Courts and the Tribunals, judges or juries involved in the cases analysed above, may not be, strictly speaking, "norms entrepreneurs[65]" but neither were they prepared to adopt, or abide by, an understanding of the Internet technology and of its "intermediaries" (neutral, global, end-to-end, escaping the necessity of spatial (jurisprudentially speaking) localization) that many may have thought were established.

Of course, there is no global jurisprudence emerging (yet), which could signal that Courts around the world are challenging the Internet actors of the first and second generation (broadly speaking the Engineers and the Corporations) and their creations. But there are a number of decisions, which are channelling "something" – misunderstanding, discomfort, fears, control, and ultimately values – that end up preventing the global cascade of the Internet norms of the first or second generations.

It may be inferred from 2014's court cases, from others in previous years and from social debates regarding Internet, that the specificities of the technology and the strong values and commitment of the first digital generations have not been enough to generate agreement (the so-called tipping point) over the norms of this radical global project, including founding a truly borderless information society.

The presence of very large corporate actors who are in a position to dominate the Internet space has radically transformed the global Information landscape. This process has involved (intentionally or not) global social and behavioural engineering, whose success was largely determined by the acceptance and internalisation of certain set of norms (eg over privacy). On the other hand, this transformative process may have fallen short of establishing an enduring normative framework[66]. Too many new and old actors; too many interests (from security to trade to innovation to education) have militated against norms cascading and tipping point. Instead, normative instability is the modus operandi.

This leads one to conclude that the next decade will be characterized by a plethora of court cases and regulatory conflicts, domestically and internationally, testing the various soft "norms" or legal principles that have been enacted and defined by the original digital power-holders[67]. From a normative standpoint, the decade ahead may well be founding cyberspace. Some would-be norms from the early years may survive. Others will simply disappear without a trace.

[65] The European Court of Justice may have come close to this role through its "right to be delinked" decision, although as explained the decision was also reflective of an older and society-driven demand.

[66] This failure may also be linked to a confused and confusing normative project on the part of Internet corporate actors, in the first place Intermediaries.

[67] These are the first generation of digital norm makers, coders and programmers initially and the large digital corporations that have developed and grown over the last decade, many of which originate from the US.