WAN IFRA
World Association of Newspapers and News Publishers

# RIGHT TO BE FORGOTTEN

## The European ruling and its extra-EU implementation

Public Affairs
Media Policy


# Public Affairs Media Policy

within WAN IFRA

# ABSTRACT

**Elena Perotti**
WAN-IFRA

Elena Perotti is Executive Director of Media Policy and Public Affairs at WAN-IFRA, the World Association of Newspapers and News Publishers. She is responsible for identifying and studying major public affairs issues within the news industry, authoring reports and articles, animating debate on social media, and educating staff and stakeholders. Elena is also in charge of interaction and liaison with WAN-IFRA's governing boards, national and regional member associations, and with many international bodies. She holds a Masters of Law in International Law and is experienced in media policy, senior management, global event organisation, and public relations.

fr.linkedin.com/in/elenaperotti

The 'Decision' rendered by the Court of Justice of the European Union in May 2014, known as the 'Ruling' that established a 'Right to be Forgotten', had the merit of bringing to global attention the importance of safeguards for the human right of privacy. In this paper I analyse in detail the specificities of the judgment, and subsequently investigate its extraterritorial implementation. A chapter is dedicated to the principles that traditionally enabled the extraterritorial enforceability of law, as well as their application in the EU Privacy Directive and in the CJEU Ruling. I conclude by proposing certain reflections on the aftermath of the 'Decision', which could constitute the starting point of a process that brings the protection of privacy forward into the new millennium.

## WAN-IFRA Public Affairs and Media Policy work:

WAN-IFRA recognises that the news publishing industry is experiencing transformation at an ever-growing pace, with new policy issues arising as the landscape changes. Much of this is related to digital publishing and the flow of information online. Our aim is to foster knowledge-sharing that allows policy experts and publishers to come together to contribute their views on where the industry is headed, and to voice the opinion of news media across the various platforms where debate on regulation and policy take place. We focus on selected policy issues, this year in particular sees us tackling privacy/the 'Right to be Forgotten' and Internet governance, with the goal of monitoring and analysing the relevant developments through our website and associated events.

WAN-IFRA is uniquely placed to represent the newspaper industry in all global policy discussions thanks the authority derived from its global newspaper membership and the legacy of 70 years spent at the service of a free press. WAN-IFRA also holds associate status to represent the newspaper industry at UNESCO, consultative status at the United Nations, the World Intellectual Property Organization, the Council of Europe and other major international bodies.

Learn more about WAN-IFRA Pubic Affairs and Media Policy work at ww.wan-ifra.org/policy

# IMPRINT

**RIGHT TO BE FORGOTTEN - THE EUROPEAN RULING AND ITS EXTRA-EU IMPLEMENTATION**

**PUBLISHED BY:**
WAN-IFRA
96b Rue Beaubourg,
75003 Paris

**CEO:**
Vincent Peyrègne

**DIRECTOR OF PUBLICATIONS:**
Dean Roper

**AUTHOR:**
Elena Perotti

**DESIGN/LAYOUT:**
Ivan Cosic & Snezana Vukmirovic, Plain&Hill

**CONTACT INFO:**
elena.perotti@wan-ifra.org
+33 1 47 42 85 00

Publishing date: 21st March 2016

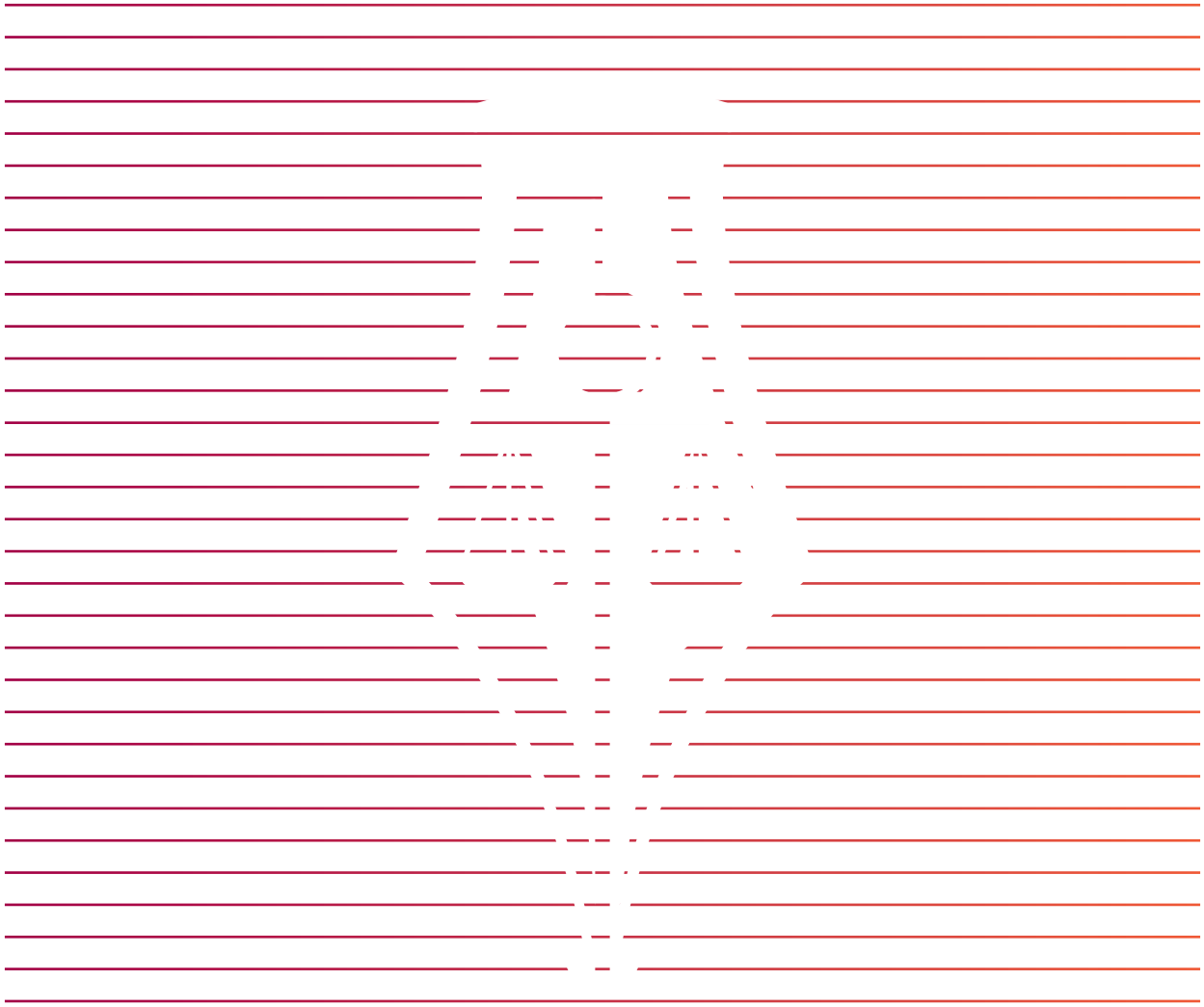


Public Affairs
Media Policy

# CONTENTS

# GOOGLE SPAIN AND GOOGLE INC V. AGENCIA ESPANOLA DE PROTECCIÓN DE DATOS (AEPD) AND MARIO COSTEJA GONZÁLEZ (C-131/12):

# DECISION AND LEGAL FRAMEWORK



# FACTS AND QUESTIONS REFERRED TO THE COURT OF JUSTICE OF THE EUROPEAN UNION

IN 2008, SPANISH NEWSPAPER LA VANGUARDIA COMPLETED ITS PIONEERING PROJECT TO PUBLISH THE ENTIRETY OF ITS ARCHIVES ONLINE. AS A CONSEQUENCE, ALL THE CONTENT EVER PRINTED IN THE NEWSPAPER SINCE 1881 BECAME SEARCHABLE ON THE INTERNET.

Mario Costeja González, a Spanish lawyer and judicial calligraphy expert, in 1998 underwent a judicial procedure that concluded with the Spanish Ministry of Labour and Social Affairs ordering La Vanguardia to include one of his properties in a real-estate auction listing aimed at the recovery of social-security debts.

Further to the digitalization of La Vanguardia archives, Mr. Costeja discovered that an Internet search on the basis of his full name returned as prominent results the two announcements regarding the forced sale of his property, published by the newspaper on 19 January and 9 March 1998.

On 5 March 2010, Mr. Costeja lodged a complaint with the Spanish data security agency Agencia Espanola de Protección de Datos (AEPD) against La Vanguardia, and against both Google Spain and Google Inc. On the grounds that "the attachment proceedings concerning him had been fully resolved for a number of years and that reference to them was now entirely irrelevant[1]", Mr. Costeja requested that La Vanguardia be ordered to alter or erase the offending pages, and that Google Spain and Google Inc. be required to take measures so that the announcements in question ceased to appear as results in an Internet search based on his name.

The AEPD rejected the complaint against La Vanguardia but upheld the one against Google Spain and Google Inc., on the grounds that search engines are to be considered data processors and therefore subject to the Spanish data-protection legislation empowering the AEDP to prohibit access to certain data[2].

1 CJEU, Case C – 131/12, Google Spain and Google Inc v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:31, paragraph 15 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131 accessed 5 October 2015. Throughout this paper, reference will be made to this judgment by using either of the following: CJEU Case C – 131/12, Costeja, the Ruling, the Decision, Google/Costeja.

2 Organic Law No 15/1999 of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088), transposing into Spanish Law Directive 95/46.

Google Spain and Google Inc. both appealed the decision before the Audiencia Nacional (National High Court), which in turn stayed the proceedings and referred to the Court of Justice of the European Union (CJEU) three questions on the interpretation of Directive 95/46 for a preliminary ruling, with the objective of clarification on whether:

1. Google is to be considered as performing, through its search, an activity of both data processing and data controlling as per Article 2(b) and (d) of Directive 95/463;

2. The territorial scope of Directive 95/46 allows for the application of the transposing national laws in the circumstances of the main proceedings and Google Spain is to be considered an "establishment" of Google Inc. within the meaning of Article 4(1)(a) of Directive 95/464;

3. The national data-protection agency is empowered to request the removal of the information directly to the search engine, without contacting the original publisher, and even when the original publication of that information was lawful and will be maintained unaltered on the web after de-linking5;

4. A data subject is enabled by the provision of the rights to erasure and blocking of data in Article 12b6, to require the de-indexing7 of web pages that are lawfully published by third parties8.

| THE RULING | |
|---|---|
| 1 | Right to be forgotten applies to results of Internet searches performed on the basis of a person's name. |
| 2 | The search results must contain data that is inaccurate, inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they are processed. |
| 3 | The search results that should be delisted on this basis might be (and remain) lawfully published in third parties websites. |
| 4 | The person's right to privacy generally overrides conflicting interest of general public in the information, unless "role played by data subject in public life" |

3 Question of the Referring Court 2 (a) and (b).

4 Question of the Referring Court 1 (a) to (d).

5 Question of the Referring Court 2 (c) and (d)

6 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, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML, accessed 10 October 2015. Article 12 of Directive 95/46, entitled 'Rights of access', provides: "Member States shall guarantee every data subject the right to obtain from the controller: ... (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data".

7 For the purpose of this publication, the terms "de-indexing", "de-linking", "de-listing", "link removal" and "search removal" are to indicate the erasure of links from search result pages, and are used interchangeably.

8 Question of the Referring Court 3.

# DECISION ON QUESTION

# A SEARCH ENGINE IS BOTH A DATA PROCESSOR AND A DATA CONTROLLER AS DEFINED IN DIRECTIVE 95/46

From the outset, it should be noted that the nature as "personal" of the data being subjected to the activity of searching, indexing and storing performed by search engines is not contested by the parties.

The Court held that the operator of a search engine shall be considered to be a "data processor" within the meaning of Article 2(b) of Directive 95/46. The Court referred to precedent decisions[9] where it held that all the operations listed in Article 2 (b) are to be considered as "processing", irrespective of the fact that the data in question were published by media sources. Furthermore, the circumstance that the data remain unaltered following the search is irrelevant towards defining the search activity as "processing", considering that the definition provided for in article 2(b)[10] lists operations that do not all require altering of personal data.

The Court also declared that the operator of an Internet search engine is to be regarded as a "controller" within the definition of Article 2 (d) of the Directive: "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data"[11].

Google Spain and Google Inc. argued that the search engine does not exercise any control on the content published by third parties, and that thus it cannot be considered to be a "controller". While addressing this argument, the decision holds that the operations performed by a search engine are distinct from the actual publication of the data on a website, and they affect the protection of that same data additionally to the operations of the publishers of websites. In the first place, the activity of indexing enables the mainstream dissemination of information that would not have been easily reachable in its original form. Secondly, the specific kind of processing established by the search engine allows for a search on the basis of a person's name to render a collection of results that constitute a "more or less detailed profile of the data subject"[12].

9 CJEU, Case C-73/07 Satakunnan Markkinapörssi and Satamedia EU:C:2008:727, paragraphs 48 and 49, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07 accessed 5 October 2015.

10 Directive 95/46, Article 2 (b): "processing of personal data" ("processing") shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

11 For the definition of "data controller" and "data processor" see Directive 95/46, Article 2 (d) and (e): "(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law; (e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

12 CJEU, Case C-131/12, paragraph 37.

# DECISION ON QUESTION

# TERRITORIAL SCOPE OF DIRECTIVE 95/46

On the question of territoriality, the Court concluded in favour of the applicability of Spanish law and jurisdiction to the main proceedings.

Having established that the activity "Google Search" constitutes both processing and controlling of personal data, the court moves to analyse whether Google Spain can be considered responsible for these activities, and therefore if Spanish law and jurisdiction apply to the proceedings. Specifically, the referring court asks whether Google Spain can be considered an "establishment", within the meaning of Article 4(1)(a) of Directive 95/46, and if the notion of "use of equipment situated on the territory of the said Member State" within the meaning of Article 4(1)(c)[13] is relevant to the case at hand.

The Court maintains that Google Spain is indeed an establishment of Google Inc. in Spain, pursuant to the wording of recital 19 in the preamble of Directive 95/46[14], and to the fact that "It is not disputed that Google Spain engages in the effective and real exercise of activity through stable arrangements in Spain"[15].

Google Spain and Google Inc. nevertheless submit that Article 4(1)(a) of Directive 95/46 is not applicable in the case, given that the activities performed by the establishment are limited to the promotion and sale of advertising space for the Spanish market, on behalf of Google Inc. Google Spain therefore would not be involved in the processing of data which is executed by Google Inc., and which as a consequence cannot be considered as "carried out in the context of" the activities of Google Spain.

After noting that with Article 4 of the Directive the European Union sought a particularly broad territorial scope, in an effort to provide effective privacy protection, and that therefore the letter of the law should be interpreted in an extensive way, the Court held that the activities of Google Search – performed by Google Inc. – and those of Google Spain are "inextricably linked". In fact, the lack of sales of local advertising would affect the profitability of Google Inc., and in turn such sale is largely made possible by the fact that Google Search allows for the targeting of the displayed advertisements so that they are relevant to each search performed[16].

13 Recital 19 reads as follows on the point: "establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements".

14 Recital 19 reads as follows on the point: "establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements".

15 CJEU, Case C-131/12, paragraph 49.

16 CJEU, Case C-131/12, paragraph 57: "As has been stated in paragraphs 26 to 28 of the present judgment, 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".

# DECISION ON QUESTION

# THE RESPONSIBILITY OF THE SEARCH ENGINE IS INDEPENDENT FROM THAT OF THE ORIGINAL PUBLISHER OF THE DATA

Google Spain and Google Inc. submit that the removal request should be addressed to the publisher of the website containing the information, by virtue of the principle of proportionality (it is less cumbersome for a publisher to proceed to the removal) and because they would allegedly be in a better position to evaluate the grounds of the request against the reason for the original publishing.

Mr. Costeja replies to this argument claiming that the data-protection authority should have the power to order the de-indexing of the information directly to the search engine, without contacting the original publisher, and the fact that the information was published lawfully and that it still appears on the original web page should have no effect.

The Court preliminarily refers to the Charter of Fundamental Rights of the European Union, which guarantees in Article 7 the right to respect for private life, and in Article 8 the right to the protection of personal data[17]. Inter alia, article 12 (b)[18] of Directive 95/46 implements those rules when it provides for the right of the data subject to obtain directly from the controller the erasure of incomplete or inaccurate data.

On the other hand, once it is established that the search engine is a data controller, it is obliged to ensure the data are processed lawfully, and that they are accurate and not excessive "in relation to the purposes for which they are collected and/or further processed[19]". Finally, as per Article 14 of the Directive, the data subject must be granted the right to object to the processing of his data, and his right to privacy needs to be balanced with the conflicting interests of third parties, as provided for in Article 7[20].

17 European Union, Charter Of Fundamental Rights Of The European Union, entry into force 1 December 2009, http://www.europarl.europa.eu/charter/pdf/text_en.pdf accessed 5 October 2015 Chapter II Freedoms, Article 7: "Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications". Article 8 Protection of personal data: "1.Everyone has the right to the protection of personal data concerning him or her. 2.Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority".

18 See *Supra,* note 6.

19 Directive 95/46, Article 6

20 Directive 95/46, Article 7: "Member States shall provide that personal data may be processed only if: ... (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data arc disclosed; or (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1)".

On the basis of this review of the applicable law, and after recalling its decision that a search on the basis of a person's name allows for the results to constitute a profile of that person, and therefore affect the data subject additionally and separately from the mere publication of that data, the Court held that the search engine may be ordered to de-link the information independently from the existence of a similar order directed to the publisher. Moreover, the data subject might in certain circumstances be unable to obtain rectification or erasure of his information from the original publisher, particularly when the original publication happened for journalistic purposes. On the other hand, the Court specified that the search engine does not benefit from the exception provided for in Article 9 of the Directive regarding "the processing of personal data carried out solely for journalistic purposes" and "necessary to reconcile the right to privacy with the rules governing freedom of expression".

SEARCH ENGINE DO NOT BENEFIT FROM THE EXCEPTION REGARDING "THE PROCESSING OF PERSONAL DATA CARRIED OUT SOLELY FOR JOURNALISTIC PURPOSES" AND "NECESSARY TO RECONCILE THE RIGHT TO PRIVACY WITH THE RULES GOVERNING FREEDOM OF EXPRESSION".

**CJEU**

# DECISION ON QUESTION

# THE DE-LINKING MAY CONCERN INFORMATION THAT IS TRUE, LAWFULLY PUBLISHED AND NOT DAMAGING

On the basis of the same reasoning developed with regard to the previous question, and further to application to the matter of the rules provided for in Articles 12 and 6 of the Directive, the search engine is subject to the obligation of link removal also when the information is true, when it remains lawfully published in a third-party website, and irrespective of whether the inclusion of that information in the results of a web search made on the basis of the data subject's name causes the latter any prejudice[21]. It pertains to the data-protection authorities or the judicial authorities to seek a balance between the rights of the data subject under Articles 7 and 8 of the Charter[22] and the interest of the general public in the availability of that information on the Internet. The Court nevertheless maintains that the rights to privacy of the data subject override as a rule the conflicting interests of the general public, and certainly the economic interests of the search engine[23]. The only exception to the prevalence of the data-subject rights mentioned by the Court is the case where the "role played by the data subject in public life" makes the general public's interest in the information preponderant[24].

21 CJEU, Case C-131/12, paragraph 92 to 96.

22 See *supra,* note 17.

23 CJEU, Case C-131/12, paragraph 81 and 97.

24 CJEU, Case C-131/12, paragraph 99.

# CONCLUSION:

# DISPELLING MYTHS ABOUT THE RULING

The news of the CJEU Ruling on Google Spain and Google Inc v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González (hereinafter "the Ruling" and "Costeja") caused strong reactions first in the press, then among the general public.

Let us summarise what the Court actually decided.

In its version contained in the Ruling, the Right to be Forgotten applies to results of Internet searches performed on the basis of a **person's name.** For that person to be granted de-linking of those results, these must contain data that is **inaccurate, inadequate, irrelevant or no longer relevant, or excessive in relation to the purposes for which they are processed.** The search results that should be de-listed on this basis might be (and remain) **lawfully published on third-party websites.**

Some of the most belligerent opinions on the Ruling appear to be largely based on misinformation: I will try to address some of those concerns here below.

## WHAT THE RULING DID NOT DO, AND WHAT IT DID INSTEAD

| THE RULING... | |
|---|---|
| **DID NOT** | **INSTEAD** |
| Create a new "Right to be Forgotten" | Defined Google as both "data processor" and "data controller"<br>• Applied existing article 12 (b) Directive 95/46<br>• Search engines generally subject to Directive provisions |
| Assign to Google the task of balancing human rights | Indicated to Audiencia Nacional criteria for balancing right to privacy and conflicting rights<br>• Google did however apply a version of those criteria in its preliminary determinations on de-linking requests |
| Pave the way for dictators who wish to revise history | The role of data subject in public life may shift the balance in favor of public's right to information<br>• But it served as inspiration for extra European laws with potential for censoring effects |
| Kill freedom of expression | Content that is de-linked from web search remains published in its original location on the Internet<br>• But it affects freedom of information<br>Exception for journalistic purposes |

## It did not create a new Right to be Forgotten

The rule that allows a data subject to request "rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data" is Article 12 (b) of the Directive 95/46, and of course it existed long before the decision of the Google/Costeja case.

What changed following the Ruling, is that search engines were declared to be data controllers, and thus subject to the Directive's provisions.

## It did not assign to Google the task of balancing human rights

It is worth remembering that the Ruling was addressed to the referring Tribunal – the Spanish Audiencia Nacional – which requested the CJEU's specific interpretation of Directive 95/46 for a preliminary Ruling. It is therefore to a judicial body that the CJEU indicated the criteria to be followed when balancing the right to privacy with other fundamental rights. But it is true that Google made the decision to anticipate possible judicial actions, and to make preliminary determinations on the de-linking requests based on the criteria outlined in the Ruling[25].

## It did not pave the way for dictators who wish to rewrit history

Various press outlets[26] have written about the fear of possible misuse of the Right to be Forgotten by politicians, criminals or shady public figures to clear the Internet slate of their offences. These fears, as far as the CJEU Ruling is concerned, are largely unjustified.

As regards public figures, the CJEU clearly stated that the interest of private subjects to the defence of their privacy would not justify the de-linking of news on grounds of Right to be Forgotten. The Court in fact excludes the search engines' obligation to de-link, in cases where the claimant plays such a role in public life "that the interference with his fundamental rights is justified by the preponderant interest of the general public in having (...) access to the information in question"[27].

On the other hand, the Ruling served indeed as inspiration for pieces of legislation adopted outside of the European Union, that could give rise to abuse from influential personalities. In July 2015, for example, Russian President Vladimir Putin signed into law a version of the Right to be Forgotten that is specifically extended to public figures. The legislation, which will come into force on 1 January 2016, indicates as a criterion for removal that the information has "become outdated due to later events or actions of the individual", and it does not apply to criminal offences[28].

---

25 See below, 2.2 "Google's implementation of the Decision".

26 As an example, see Robert Peston, "Why has Google cast me into oblivion?", BBC News Business, 2 July 2014 http://www.bbc.com/news/business-28130581, accessed 5 October 2015. In the article dated 2 July 2014, the author claims that one of his articles was censored by Google at the request of a person well-known in the world of investment banking. After further investigation, it was discovered that the person who asked and obtained the de-linking was in fact one who had commented the article. Other examples: David Lee, "Google ruling 'astonishing', says Wikipedia founder Wales", BBC News Technology, 14 May 2014, http://www.bbc.com/news/technology-27407017 accessed 5 October 2015. Wales defined the ruling as "one of the most wide-sweeping Internet censorship rulings that I've ever seen". James Ball, "'Right to be forgotten' ruling creates a quagmire for Google et al", The Guardian, 13 May 2014, http://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google accessed 5 October 2015: "either an eerie parallel with China's domestic censorship of search results, or a huge incentive for tech investment to get the hell out of Europe".

27 See *supra,* 1.5 "Decision on Question 4): the de-linking may concern information that is true, lawfully published and not damaging".

28 Vera Shaftan, "Russia signs controversial 'right to be forgotten' bill into law", http://www.dataprotectionreport.com/2015/07/russia-signs-controversial-right-to-be-forgotten-bill-into-law/, accessed 6 October 2015.

## It did not kill freedom of expression

The content that is de-linked from a Google search remains published in its original location on the Internet. The only thing that changes is the impossibility to reach that information through a search based on the name of the specific person to whom the request of de-listing was granted: a different query will still lead to that content. Of course, doubts remain on the effect that de-listing has on the Freedom of Information, as the ability to reach a de-indexed piece of news is undoubtedly reduced. In addition, it was rightfully noted[29] that "While the target of the search might be a European citizen or resident, one cannot exclude the possibility that this person is of interest to the constituents of other States".

Another important myth to dispel is the one regarding alleged repercussions on journalism in general. While motivating its decision that the responsibility of a search engine shall be entirely independent from that of the original publisher of the information (read "news" in this case), the Court rightfully referred to the existence of an exception for journalism purposes[30], which exempts news publishers from the respect of Article 12 (b), or, as it is now known, the Right to be Forgotten. For the same reason, it seems unlikely that the CJEU would ever apply in the future this rule directly to archives of newspapers.

## It did not make decisions on the territorial reach of the de-listing

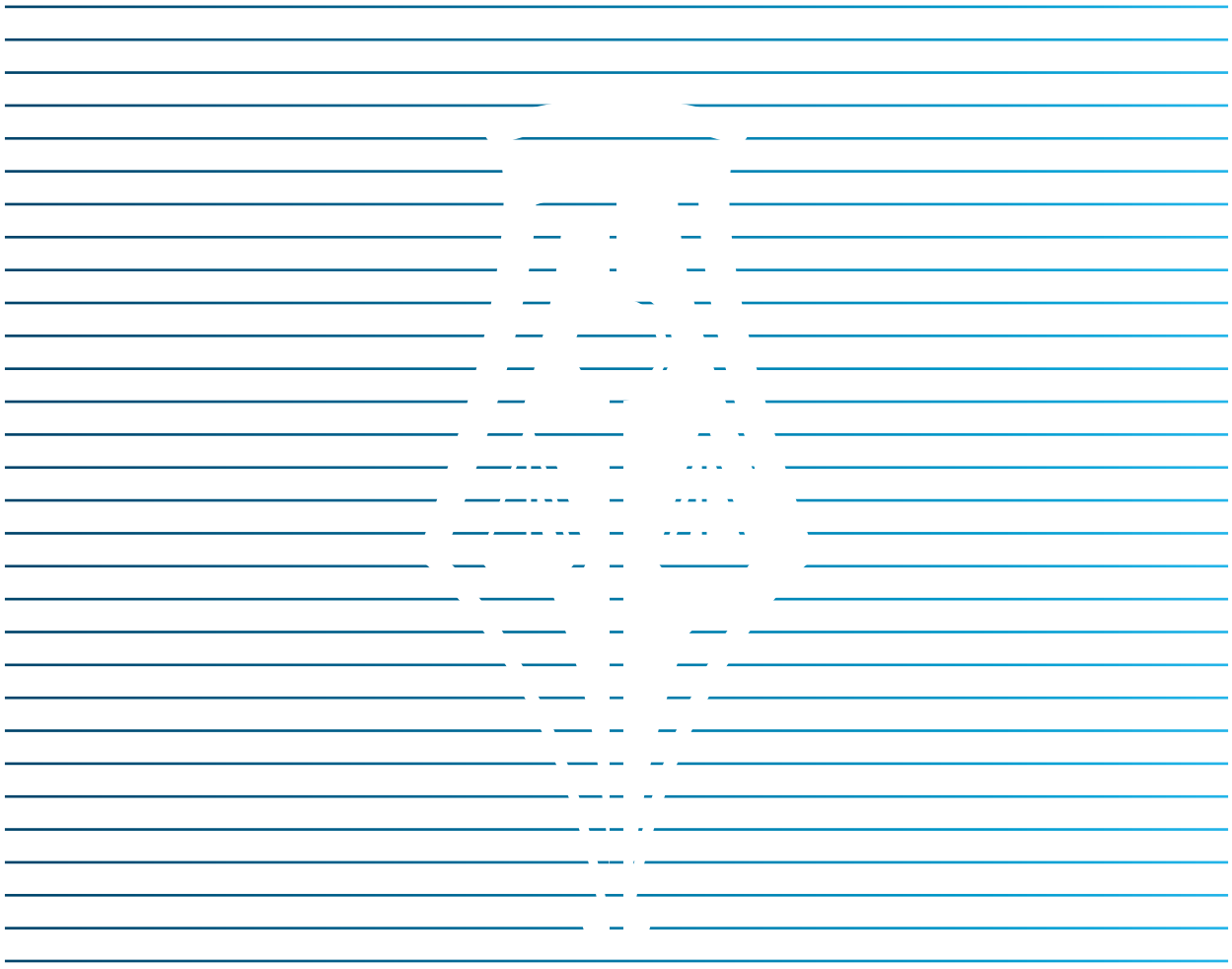
The CJEU was silent about this topic. It did not suggest that search engines should limit the implementation of the Ruling to specific websites or areas, nor did it explicitly require a global de-linking.

However, the Court opened the way to establishing extraterritorial jurisdiction on Google Inc. through its interpretation of Article 4 of the Directive that leads to the conclusion that Google Spain represents an "establishment" of Google Inc., and that the latter's search activities are "carried out in the context" of the activities of Google Spain. It infers from Google's declarations that the entirety of the search – read the "data-controlling" – activity is performed outside of Spain: the fact that the Court found Google Inc. and Google Spain "inextricably linked" allows for the extension of Spanish legislation and jurisdiction to that extra-European activity.

29 B. Van Alsenoy and M. Koekkoek, "The extraterritorial reach of the EU's 'right to be forgotten'", ICRI Working Paper 20/2015, 19 January 2015, 16 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551838 accessed 7 October

30 Directive 95/46 Article 9. See also *supra*, 1.4 "Decision on Question 3): the responsibility of the search engine is independent from that of the original publisher of the data".

# THE QUESTION OF EXTRATERRITORIALITY IN THE IMPLEMENTATION OF THE CJEU RULING



# INTERPRETATION OF THE DECISION FROM ARTICLE 29 DATA PROTECTION WORKING PARTY

Article 29 Data Protection Working Party[31] (WP29) was established by Article 29 of the Directive 95/46, from which it derives its name. It is an independent European advisory body on data protection and privacy, which comprises all the data protection authorities from the countries that are part of the European Union, the European Data Protection Supervisor[32] and the European Commission.

Following a meeting organised with Google, Microsoft and Yahoo! in June 2014, and the answers of the three US-based firms to a public questionnaire, Article 29 on 26 November 2014 adopted guidelines[33] on the implementation of the Ruling as well as the criteria to be used by the national data protection authorities (DPAs) when addressing complaints. On the matter of territoriality, the guidelines read in Article 7 that "limiting the de-listing to EU domains (...) cannot be considered a sufficient mean to satisfactorily guarantee the rights of data subjects according to the Ruling", and that "in any case de-listing should also be effective on all relevant domains, including .com"[34]. They also clarify, *ratione personae,* that DPAs should focus on requests originating from the European territory: "Article 8 of the EU Charter of Fundamental Rights [...] recognises the right to data protection to "everyone". In practice, DPAs will focus on claims where there is a clear link between the data subject and the EU, for instance where the data subject is a citizen or resident of an EU Member State"[35].

31 The tasks of Article 29 Working Party are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

32 The European Data Protection Supervisor is an authority established on the basis of Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000. The Supervisor is appointed by common accord of the EU Parliament and Council for a term of five years, on the basis of a list drawn up by the Commission following a public call for candidates. The Supervisor monitors the EU administration's processing of personal data, advises the European Commission, the European Parliament and the Council on policies and legislation that affect privacy and cooperates with similar authorities to ensure consistent data protection, particularly through the platform of the Article 29 Working Party. The incumbent is Giovanni Buttarelli, appointed for a five-year term on 4 December 2014.

33 Article 29 Data Protection Working Party, "Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, accessed 3 October 2015

34 *Ibid.,* paragraph 20.

35 Ibid., paragraph 19.

# GOOGLE'S IMPLEMENTATION OF THE DECISION

It should preliminarily be noted that Google has for several years been implementing mechanisms of links takedown[36]. Before the judgment, Google already had a system in place to handle deletion requests of private data such as national identification numbers, bank account numbers, credit card numbers or images of signatures.

The novelty introduced by the Ruling was the fact that since May 2014 the de-linking requests connected to a much wider range of data protection joined the bulk of existing claims, which mainly referred to copyright infringement, antitrust, defamation etc. In addition, since the Ruling, the illegality of the content is no longer the main aspect to be taken in consideration, and Google's responsibility is, in matters of privacy, disconnected from that of the publisher.

LINK TAKEDOWNS ARE NOT NEWS AND WERE NEVER LIMITED TO RIGHT TO BE FORGOTTEN COMPLAINTS: GOOGLE PERFORMS ROUGHLY 1.6 MILLION LINK REMOVALS PER DAY, WITH 50 MILLION IN AUGUST 2015 ALONE.

Following the CJEU decision on the Costeja case, Google determined, rather than awaiting case-by-case rulings from data protection or judicial authorities, to be proactive in relation to the implementation of the Ruling. It started by launching an official request process for URL removal based on privacy claims on 29 May 2014, 13 days after the Ruling. It then organised an Advisory Council[37] composed of eight European scholars and figures of the publishing industry, that toured Europe for six months with the declared objective of gathering input from Europeans. The task was to "advise (Google) on performing the balancing act between an individual's right to privacy and the public's interest in access to information"[38].

In February 2015 the Advisory Council rendered its report to Google, identifying the details of four criteria on which de-listing requests should be evaluated: the role of the person in public life, the nature of the information that is the object of the request, the source of original publishing, and the time elapsed.

36 According to a source within Google, interviewed in September 2015, the link removals performed by Google are roughly 1.6 million per day, with 50 million in August 2015 alone.

37 https://www.google.com/advisorycouncil/ accessed 7 October 2015.

38 Report of the Advisory Committee to Google on the Right to be Forgotten, 22 February 2015, 1, http://www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf accessed 7 October 2015.

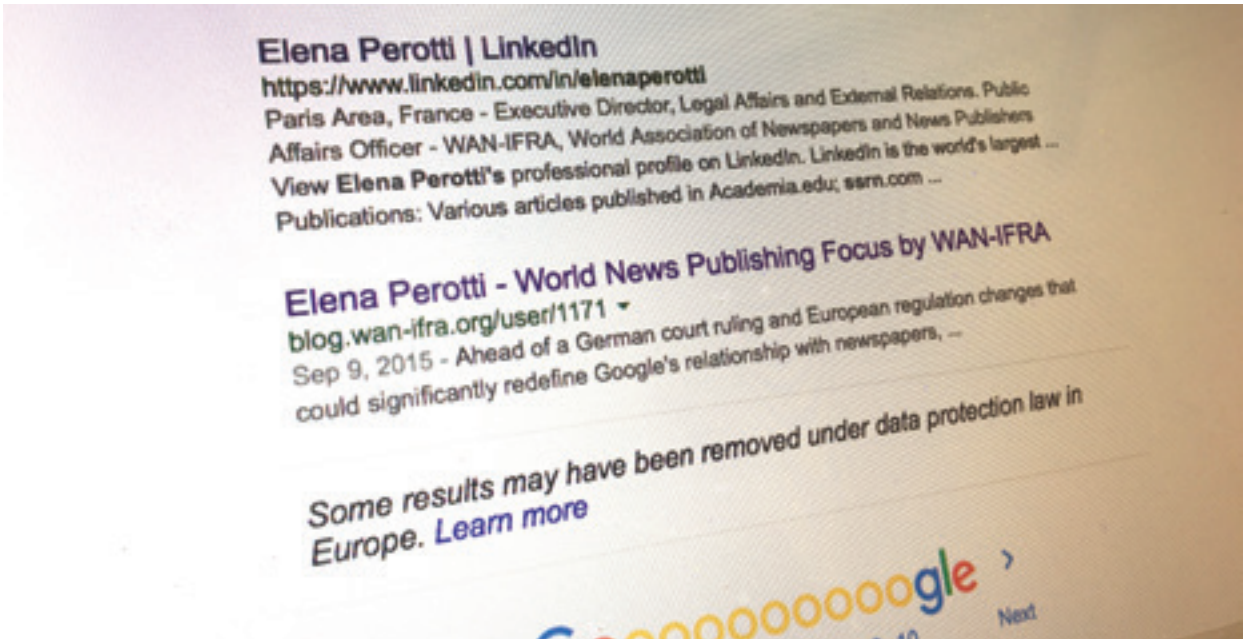
The Council covered the matter of geographic scope of de-listing in paragraph 5.4 of their report. It approved the decision made by Google to expand to the whole of the European domains the effects of granted de-linking[39], in consideration of the authority of the CJEU across Europe, and of the fact that more than 95% of searches performed in the European countries appear to be redirected to the national versions of the engine.

Regarding the opportunity of global de-indexing, the Council considered that "there is a competing interest on the part of users outside of Europe to access information via a name-based search in accordance with the laws of their country". The Council concluded that, given concerns of proportionality, "de-listings applied to the European versions of search will, as a general rule, protect the rights of the data subject adequately in the current state of affairs and technology"[40].

To date, Google evaluated for removal 1,152,540 URLs, based on 324,094 requests received, and it performed de-linking in 41.8% of the cases submitted[41].

In July 2015, The Guardian published a piece[42] unveiling leaked data on Google's internal statistics regarding Right to be Forgotten de-linking requests, and their outcome. The data in question, even though presented by some press as surprising, seem to be in line with the recommendations of the CJEU: "95% of Google privacy requests are from citizens out to protect personal and private information", and only 5% of the people who required de-linking did so in relation to criminal activity, or to public figures.

Today, a search performed on a European Google domain on the basis of a name will most likely return results indicating, at the bottom of the page, the warning "Some results may have been removed under data-protection law in Europe", with a link to frequently asked questions about the Ruling and its implementation.




39 See Peter Fleischer, "Response to the Questionnaire addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the 'right to be forgotten'", 31 July 2014, https://docs.google.com/file/d/0B8syaai6SSfiTOEwRUFyOENqR3M/edit?pli=1 accessed 7 October 2015.

40 Report of the Advisory Committee to Google on the Right to be Forgotten, 19.

41 Source: Google Transparency Report https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en accessed 7 October 2015.

42 Sylvia Tippmann and Julia Powels, "Google accidentally reveals data on 'right to be forgotten' requests", The Guardian, 14 July 2015, http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests, accessed 7 October 2015.

# REACTIONS OF NATIONAL DPAS TO THE TERRITORIAL SCOPE OF THE RULING IMPLEMENTATION

## THE FRENCH CNIL

In April 2015, the French DPA, the Commission Nationale de l'Informatique et des Libertés (CNIL), officially requested[43] Google to de-list search results that breach data protection in all domains globally. The agency declared that "in order to be effective, delisting must be carried out on all extensions of the search engine and that the service provided by Google search constitutes a single processing", and thus addressed to Google formal notice to proceed within 15 days.

Google responded through a blog post signed by Peter Fleischer, Google's Global Privacy Counsel, who refused to comply on grounds that if the law of one region were to be applied to the whole world, "the Internet would only be as free as the world's least free place"[44].

CNIL President Isabelle Falque-Pierrotin rejected this appeal on 21 September[45]: Google could now be subject to administrative sanctions, and also face criminal prosecution.

"THE INTERNET WOULD ONLY BE AS FREE AS THE WORLD'S LEAST FREE PLACE"

**PETER FLEISCHER,**
GOOGLE'S GLOBAL PRIVACY COUNSEL

43 Commission nationale de l'informatique et des libertés, "CNIL orders Google to apply delisting on all domain names of the search engine", 12 June 2015, http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/ accessed 7 October 2015.

44 Peter Fleischer, "Implementing a European, not global, right to be forgotten", 30 July 2015, http://googlepolicyeurope.blogspot.fr/2015/07/implementing-european-not-global-right.html accessed 7 October 2015. Google's appeal was sustained by various voices in the press, including a coalition led by Reporters Committee for Freedom of the Press: https://www.rcfp.org/reporters-committee-leads-coalition-urging-french-data-regulator-reconsider-right-be-forgotten-delis

45 Specifically on the matter of extraterritoriality, CNIL nods to the effects theory (see below, 3.2.2 and 3.4.2) when it declares "this decision does not show any willingness on the part of the CNIL to apply French law extraterritorially. It simply requests full observance of European legislation by non European players offering their services in Europe." Commission nationale de l'informatique et des libertés, "Right to delisting: Google informal appeal rejected", 21 September 2015, http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/ accessed 7 October 2015.

# THE ENFORCEMENT NOTICE OF THE BRITISH ICO

On 18 August 2015, the British DPA, the Information Commissioner's Office (ICO) ordered[46] Google Inc. to remove nine links to current news stories recently appeared in the media regarding the de-indexing granted to older articles. Having granted the removal of links to the original information, Google resisted de-linking the new articles reporting the story of the removal itself, which appears following a search on the basis of the complainant's name.

Google argued that the articles in question "formed an essential part of a recent news story", and that it "took into account the news media's journalistic judgments in determining whether the information was relevant and in the public interest[47]".

As regards specifically the matter of territoriality, the ICO echoed the Ruling when it declared itself "satisfied that the processing of personal data (...) is carried out in the context of the commercial and advertising activity of Google Inc.'s establishment in the UK". The ICO then proceeded to apply the British Data Protection Act – which implements in the United Kingdom Directive 95/46 – and ordered the American company[48] to remove the offending links. Google had 35 days to respond, which I am told they did: the details of the proceeding are confidential and undisclosed.

46 Data Protection Act 1998 Supervisory Powers of the Information Commissioner Enforcement Notice dated 18 August 2015, https://ico.org.uk/media/action-weve-taken/enforcement-notices/1432380/google-inc-enforcement-notice-18082015.pdf accessed 7 October 2015.

47 *Ibid.*, paragraph 19.

48 In paragraph 27 of the Enforcement order ICO specified that it did not dispute the journalistic interest in the story, and its relevance for the general public, but it held that such interest could be met without need for a search made on the basis of the complainant's name pointing to that news.

# IMPLEMENTATION OF THE RULING BY JUDICIAL AUTHORITIES: CANADA, THE EQUUSTEK CASE

Since the CJEU decision on 13 May 2014, it appears that judges in different parts of the world are being "inspired" by the Ruling – when establishing the obligation on the part of search engines to restrain access to links – in a form of "migration (...) of ideas that might be perceived as universal"[49].

The examples within the European Union understandably number quite a few[50], but the Equustek case, discussed in Canada, is particularly interesting both for its location literally on the other side of the world, and for its faithful application of the principles of Costeja.

The case[51] (hereinafter Equustek) regarded plaintiff Equustek Solutions, a manufacturer of networking devices. Equustek was fighting the defendants' practice of advertising Equustek Solutions products on the Internet, while sending to customers their own competing products instead. Following several judicial actions and subsequent court orders to cease their deceptive practices, the defendants brought their business entirely online, and started operating through a network of websites. Google complied with Equustek's requests to remove the defendants' 345 URLs from search results on Google.ca, but refused to do so on its other domains.

The plaintiff sought an interim order against Google Inc., which was not a party in the proceedings.

When analysing its territorial competence, the Supreme Court of British Columbia noted that neither Google Inc. nor Google Canada were incorporated in British Columbia. Google.ca is in fact incorporated in Nova Scotia, and Google Inc. in Wilmington, Delaware, with its head office in Mountain View, California.

The Court therefore moved to considering the facts in light of the provisions of the Court Jurisdiction And Proceedings Transfer Act, Chapter 28 (hereinafter CJPTA), which in Article 1 states that "territorial competence means the aspects of a court's jurisdiction that depend on a connection between (a) the territory or legal system of the state in which the court is established, and (b) a party to a proceeding in the court or the facts on which the proceeding is based"[52]. In

49 For an innovative approach in Internet law studies through the analysis of global Courts interaction based on judicial dialogue see Krystyna Kowalik-Bańczyk, Oreste Pollicino, "Migration of European judicial ideas concerning jurisdiction over Google on withdrawal of information", in course of publication, Yearbook of European Law, 2015.

50 See in particular, for France, Tribunal de Grande Instance de Paris, Ord. de réf., 16 September 2014, M. et Mme X et M. Y / Google France, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291 accessed 11 October 2015, where interestingly enough Google France was sentenced to take charge of global de-linking of defaming website in Google Inc.; and Tribunal de Grande Instance de Paris, Ord. de réf., 19 December 2014, Marie-France M. / Google France et Google Inc. http://junon.univ-cezanne.fr/u3iredic/?p=16671 accessed 11 October 2015, where the Court considered that eight years were enough to make the plaintiff's conviction for fraud "irrelevant" and thus forgettable, irrespective of the fact that said plaintiff could be considered a "public figure" having run for local elections only the year before the decision. For an overview of European cases referencing Costeja, see Reflets, "Développements juridiques présentant un intérêt pour l'Union européenne », N 1/2015, http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-03/fr_2015_reflets1.pdf accessed 11 October 2015.

51 Equustek Solutions Inc. v. Jack, 2014 BCSC 1063 (CanLII), http://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.html accessed 8 October 2015.

52 British Columbia, Statutes and Regulations, Court Jurisdiction And Proceedings Transfer Act [Sbc 2003] Chapter 28, http://www.canlii.org/en/bc/laws/stat/sbc-2003-c-28/latest/sbc-2003-c-28.html accessed 8 October 2015.

Article 10, the CJPTA indicates the cases when a "real and substantial connection" is presumed to exist between the facts of a proceeding and British Columbia[53], and lists among others the situations where a "business carried on in British Columbia" is concerned[54].

The reasoning followed by the Canadian Court to establish its territorial jurisdiction has several points in common with that of the CJEU in the Costeja case.

It first considered the different activities performed by Google Inc. and Google.ca, one dedicated to Internet search, the other mainly to collecting advertising aimed at the Canadian public. The Court then noted that "Google's advertising success is driven by the very high quality of its search results.[55]"

"(THE FACT ) THAT THIS ANALYSIS WOULD GIVE EVERY STATE IN THE WORLD JURISDICTION OVER GOOGLE'S SEARCH SERVICES (...) FLOWS AS A NATURAL CONSEQUENCE OF GOOGLE DOING BUSINESS ON A GLOBAL SCALE, NOT FROM A FLAW IN THE TERRITORIAL COMPETENCE ANALYSIS"

**SUPREME COURT OF BRITISH COLUMBIA**

Google contended that if the simple fact of citizens being enabled to perform a search on its engine established a connecting factor with a Country, then every civil Court in the world could assert jurisdiction over Google in respect of search results. It added that "its programs automatically generate search results without Google being actively involved in the particular search[56]".

In its argument, Google relied on the judicial precedent of Van Breda[57], a ruling often relied upon in matters concerning the conflict of laws in Canada. The Canadian Court examined the Van Breda decision together with other two precedents, one Canadian, the second American, all establishing that the mere existence of a website accessible from the territory was not a sufficient connecting factor[58].

53 Ibid., Article 10 : Real and substantial connection: Without limiting the right of the plaintiff to prove other circumstances that constitute a real and substantial connection between British Columbia and the facts on which a proceeding is based, a real and substantial connection between British Columbia and those facts is presumed to exist if the proceeding: (a) is brought to enforce, assert, declare or determine proprietary or possessory rights or a security interest in property in British Columbia that is immovable or movable property, ... (h) concerns a business carried on in British Columbia.

54 Moreover, the order sought by the plaintiff against Google is aimed at enforcing his intellectual property rights, what the Court identifies as "movable rights" and therefore a connecting factor in the definition of Article 10 CJPTA, letter (a), see *Supra,* note 54.

55 Equustek, paragraph 33. Similarly, see Costeja, paragraph 57.

56 Equustek, paragraph 47.

57 Club Resorts Ltd. v. Van Breda, [2012] 1 SCR 572, 2012 SCC 17 (CanLII), http://www.canlii.org/en/ca/scc/doc/2012/2012scc17/2012scc17.html accessed 8 October 2015.

58 Respectively Thumbnail Creative Group Inc. v. Blu Concept Inc., 2009 BCSC 1833 (CanLII) http://www.courts.gov.bc.ca/jdb-txt/SC/09/18/2009BCSC1833.html , and Zippo Manufacturing v. Zippo Dot Com Inc., 952 F. Supp. 119 (W.D. Pa. 1997) http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.html, both accessed 8 October 2015.

The Court held that Google search is not a "passive information site", because the results are tailored on the user's search history and interests[59]. Moreover, Google.ca actively sells advertising to companies established in British Columbia, which establishes an additional connection with the territory. When Google argued, just like in the Costeja case, that its search and advertising activities are distinct, the Court countered on the basis of arguments very similar to those sustained by the CJEU in the Costeja case, which was explicitly mentioned. Indeed, it noted that the advertisements showed alongside the search results are "contextual", meaning that they are determined by a combination of the search topic and the specific previous behaviour of that user. The Court concluded that the advertising and search activities are, in the Google business model, "inextricably linked"[60].

The Court also considered that one of the two interlinked activities had undeniably a weaker relation with British Columbia, but held that this does not affect the Court's territorial competence. Directly addressing Google's objection, the Court added: "(the fact ) that this analysis would give every state in the world jurisdiction over Google's search services (...) flows as a natural consequence of Google doing business on a global scale, not from a flaw in the territorial competence analysis"[61].

After finding in favour of its jurisdiction on the matter, the Canadian court held that a measure limited to the domain Google.ca would not suffice to defend the interests of the plaintiff, given the existence of the other Google domains. It therefore issued an injunction restraining Google from including in its search results across the world the contested websites. The ruling was upheld by the Court of Appeal of British Columbia on 23 July 2014.

**IMPLEMENTATION BY COURTS: CANADA, THE EQUUSTEK CASE**

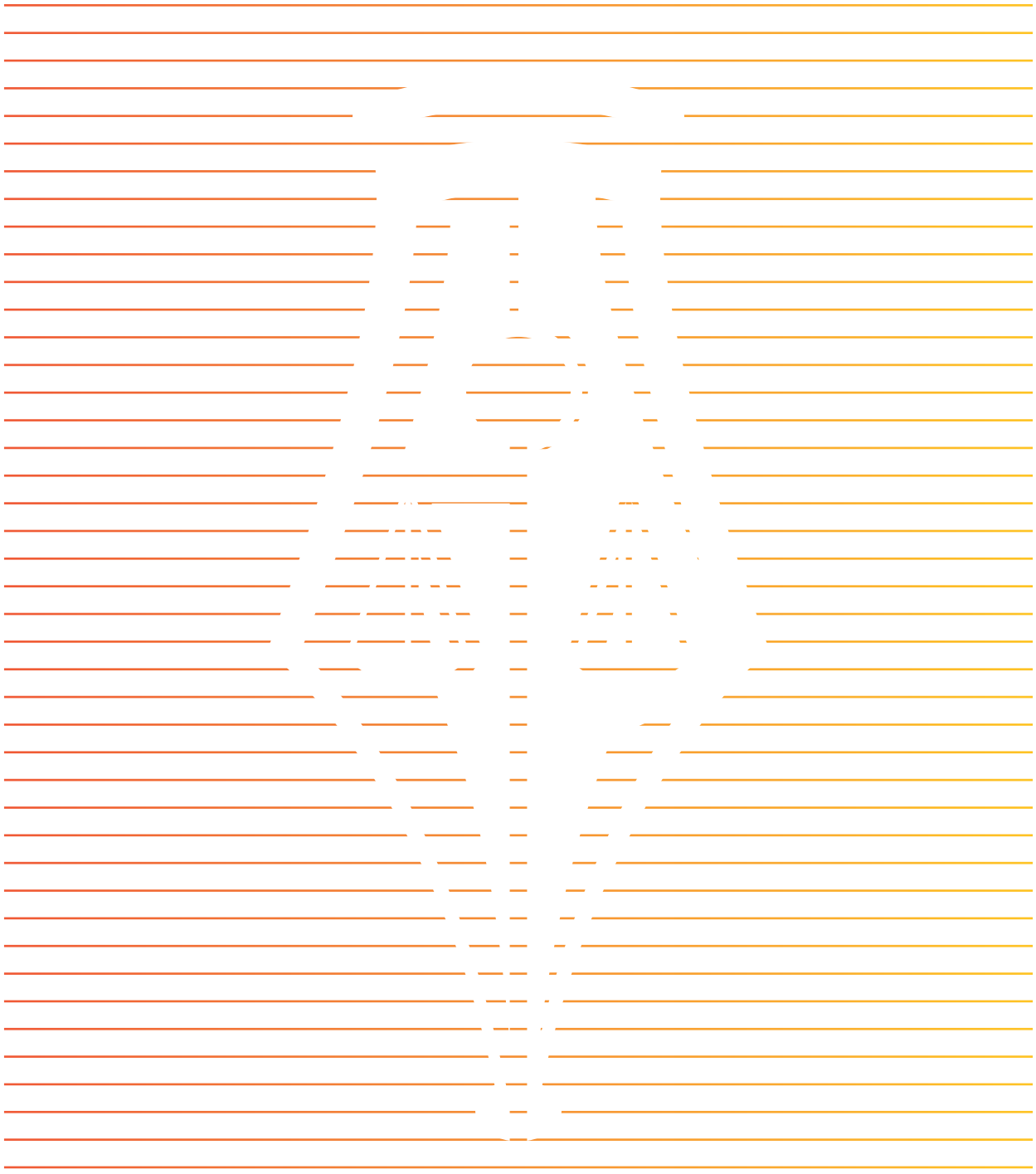
| **Google** | **Supreme Court British Columbia** |
|---|---|
| Search results are automatically generated | Contextual advertising: not a passive information site |
| Google Inc. and Google Canada perform different activities | Google's advertising success driven by very high quality of search results: **inextricably linked** |
| If ability of citizens to search were enough to connect, every court in the world could assert jurisdiction | Natural consequence of doing business on global scale, not flaw of territorial competence analysis |
| Real & substantial connection established/Injunction to Google Inc. to exclude contested websites form search results across the world | |

59 For a diametrically opposite conclusion – but in a defamation case, with very different premises – see Supreme Court of British Columbia, Niemela v. Malamas, 2015 BCSC 1024 (CanLII) http://canlii.ca/t/gjk4w accessed 10 October 2015. The Canadian Court held that Google search algorithm was a "passive instrument" which is unaware of the content of the websites identified in the search results. The Court concluded that "Google does not authorise the appearance of the snippets on the user's screen in any meaningful sense but has merely, by the provision of its search service, played the role of a facilitator".

60 Equustek, paragraph 63 and Costeja, paragraph 56.

61 Equustek, paragraph 64.

# EXTRATERRITORIAL ENFORCEABILITY OF LAW



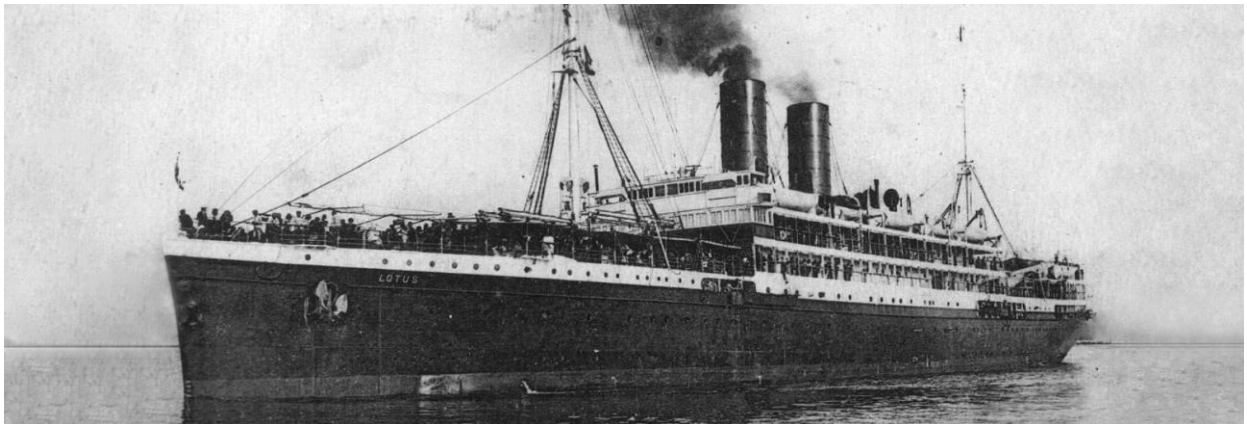
# INTRODUCTION: TERRITORIALITY AND EGGS

Imagine that at the beginning of time, hens laid only yellow, blue and red eggs, and that industries were created with exclusive competence on each colour. As an effect of interbreeding, "primary colour" hens would occasionally lay orange or purple eggs, which would be assigned to one industry or another following long discussions on the exact shades, and sometimes unilateral declarations of competence.

Suddenly it happened that hens could be fertilised through the air, interbreeding increased dramatically the number of non-primary coloured eggs, and it became a challenge to define which eggs belonged to which industry. High walls were built around the primary industries, meetings at the highest level were organised, university classes were taught, many books were written. Some suggested the creation of a new overreaching industry, which would deal with all the funny-coloured eggs. In the end, much before a solution could be found, all eggs ended up white or brown, and all the industries lost their competence.

Similarly, the advent of the Internet has multiplied the cases where transnational events are created, which are "coloured" with shades belonging to a multitude of different States, not "quite French, Japanese or Australian, but a bit of each"[62]. The rules based on location that for centuries have allowed for the assignation of international events to one State or another are rarely applicable in a straightforward way. The territoriality-based system is therefore facing challenges that need to be addressed in innovative ways. In this chapter, I will first examine a few of the traditional principles used for establishing extraterritorial jurisdiction, and then analyse how these were adapted in the context of EU privacy law, and the Ruling.

62 *Ibid.*, 3.




# JURISDICTION IN INTERNATIONAL LAW: THE LOTUS CASE PRINCIPLES

The universally accepted extent of a State's prescriptive jurisdiction, or its right to create, amend or repeal legislation, is "the territory over which the State is sovereign"[63]. Only international agreements or rules of Customary International Law[64] can enable a State to extend and enforce its legislation outside its borders.

In the absence of an International convention that regulates the extraterritorial exercise of prescriptive jurisdiction and its relation with other States sovereignty, Customary International Law assists in identifying a series of rules on the topic.

The traditional cornerstone[65] of this body of Customary Law is the decision rendered in 1927 by the Permanent Court of International Justice (PCIJ)[66] in the so-called Lotus case[67].

---

63 Antonio Cassese, "International Law", Oxford University Press; 2nd edition (10 February 2005), 29.

64 Customary International Law is one of the sources of law as identified by Article 38 (1) (b) of the International Court of Justice Statute http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0. It results from international obligations arising from established general and consistent practice of states that they follow from a sense of legal obligation, as opposed to obligations arising from international treaties. Customary International Law has a subjective element that was defined by the ICJ as follows: "Not only must the acts concerned amount to a settled practice, but they must also be such, or be carried out in such a way, as to be evidence of a belief that this practice is rendered obligatory by the existence of a rule of Iaw requiring it. The need for such a belief, i.e. the existence of a subjective element, is implicit in the very notion of the *opinio juris sive necessitatis*. The States concerned must therefore feel that they are conforming to what amounts to a legal obligation", ICJ, North Sea Continental Shelf Cases, 20 February 1969, paragraph 77 http://www.icj-cij.org/docket/files/51/5535.pdf. Article 38 (1) of the ICJ Statute defines the sources of International Law as follows: "Article 38 1: The Court, whose function is to decide in accordance with international law such disputes as are submitted to it, shall apply: a. international conventions, whether general or particular, establishing rules expressly recognised by the contesting states; b. international custom, as evidence of a general practice accepted as law; c. the general principles of law recognised by civilised nations; d. subject to the provisions of Article 59, judicial decisions and the teachings of the most highly qualified publicists of the various nations, as subsidiary means for the determination of rules of law".

65 See Dan E. Stigall, International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law, Hastings International and Comparative Law Review, Vol. 35, No. 2, p. 323, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043287 accessed 10 October 2015. The author reports that the PCIJ ""reaffirmed the enduring force of this rule as recently as 2010, noting that the rule articulated in *Lotus* remains a cornerstone of the international law of jurisdiction".

66 The Permanent Court of International Justice (PCIJ) is the predecessor of the International Court of Justice (ICJ). See official presentation of ICJ at http://www.icj-cij.org/court/index.php?p1=1 "The International Court of Justice (ICJ) is the principal judicial organ of the United Nations (UN). It was established in June 1945 by the Charter of the United Nations and began work in April 1946. The seat of the Court is at the Peace Palace in The Hague (Netherlands). Of the six principal organs of the United Nations, it is the only one not located in New York (United States of America). The Court's role is to settle, in accordance with international law, legal disputes submitted to it by States and to give advisory opinions on legal questions referred to it by authorised United Nations organs and specialist agencies. The Court is composed of 15 judges, who are elected for terms of office of nine years by the United Nations General Assembly and the Security Council. It is assisted by a Registry, its administrative organ. Its official languages are English and French".

67 S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (7 September) http://documents.law.yale.edu/sites/default/files/SS%20Lotus%20-%20PCIJ%20-%201927.pdf accessed 10 October 2015.

In 1926, a collision on the high seas between the French mail steamer Lotus and the Turkish coal cargo ship Boz-Kourt caused the latter to sink and eight Turkish citizens to die. The captain of the French vessel was arrested, tried and convicted in Turkey. The PCIJ was called upon to establish whether Turkey had a right to extend its jurisdiction to the French national.

The Lotus case is considered a landmark because it established a series of principles that are still at the basis of extraterritorial prescriptive jurisdiction.

## THE PRINCIPLE OF TERRITORIAL JURISDICTION

A State cannot exercise its jurisdiction in the territory of another State, unless a rule of International Law allows for this extension.

"Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention[68]".

## EXTENSION OF TERRITORIAL JURISDICTION: THE EFFECTS THEORY

A State can exercise its jurisdiction in its own territory over a foreign national for conduct that took place abroad and produces effects within his territory, unless a rule of International Law prohibits this, even in absence of a specific permitting rule[69].

The Court held that independent States agree upon "restrictions" of their sovereignty through the exercise of their will and discretion, when abiding to international usages and agreeing to conventions: no restrictions can be presumed on the basis of the absence of rules[70].

---

68 PCIJ, Lotus decision, page 18 and 19.

69 Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, (International Law) leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable... In these circumstances all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty". *Ibid.,* page 19.

70 This concept expressed in the Lotus case, which can be extended to assume that all that is not specifically forbidden is to be considered allowed under International Law, is now sometimes challenged by part of the International Law community, which observe that in similar circumstances it would be preferable to define what the law allows, rather than limit the analysis to what it does not forbid. For an authoritative comment on this matter, and the subsequent evolutions in the Law of the Sea, see Malcolm Shaw, International Law, 2008, Sixth Edition, Cambridge University Press, 656, https://www.academia.edu/3386070/Malcolm_N._Shaw_-_International_Law_6th_edition_2008, accessed 18 October 2015. One famed example of this inclination, can be found in the dissenting opinion of Judge Yusuf in the ICJ Advisory Opinion "Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo", I.C.J. Reports 2010, p. 403, accessible online at http://www.icj-cij.org/docket/files/141/15987.pdf. On 17 February 2008 the Provisional Institutions of Self-Government of Kosovo declared independence from Serbia. The General Assembly of the United Nations requested the International Court of Justice to render an advisory opinion on whether the unilateral declaration of independence was in accordance with international law. The Court concluded that "general international law contains no applicable prohibition of declarations of independence." (paragraph 84). Notwithstanding his favourable vote, Judge Abdulqawi Yusuf from Somalia appended to the decision a dissenting opinion, where he reproached the ICJ for having reduced the question to whether the Declaration of Independence was prohibited by International Law. Judge Yusuf writes that the Court missed an invaluable opportunity to take a wider approach to the question, and rather establish "whether that process could be considered consistent with international law in view of the possible existence of a positive right of the people of Kosovo in the specific circumstances which prevailed in that territory". Separate Opinion of Judge Yusuf, "I Introduction" and "II. The Scope And Meaning Of The Question Put To The Court", particularly pages 220 and 225, http://www.icj-cij.org/docket/files/141/16005.pdf.

"Offences, the authors of which at the moment of commission are in the territory of another State, are nevertheless to be regarded as having been committed in the national territory, if *one of the constituent elements of the offence, and more especially its effects,* have taken place there[71]". In the Lotus case, the Boz-Kourt, where the effects of the offence were felt, was equated to Turkish territory.

The effects principle is widely applied in antitrust law, when States regulate foreign activities that impact competition in their markets.

## SUBJECTIVE TERRITORIAL JURISDICTION OR PASSIVE PERSONALITY PRINCIPLE

In this particularly controversial theory[72], a State asserts jurisdiction over injuries to their nationals committed abroad.

In the Lotus case, this principle is treated as a corollary to the effect theory, in that the act of negligence committed by the foreigner abroad resulting in the death of Turkish nationals represented a "constituent element of the offence", meaning that without the death of the Turkish nationals, the offence would have not taken place. "These two elements are, legally, entirely inseparable, so much so that their separation renders the offence non-existent"[73].

Essentially, the Court managed to bring the argument back to the effects theory, without needing to take a specific position with respect to the passive personality principle[74].

71 PCIJ, Lotus decision, page 23, emphases added.

72 For an analysis both of the reasons of controversy, and of the limits within which the theory was in fact used in the Lotus case, see Arthur Lenhoff, "International Law and Rules on International Jurisdiction", Cornell Law Review, Vol. 50, Fall 1964, 10, http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2435&context=clr accessed 10 October 2015.

73 PCIJ, Lotus decision, page 18.

74 For an interesting argument on the differences and similarities between the Lotus case and that of Italian vessel Enrica Lexie, see Duncan Hollis, "The Case of Enrica Lexie: Lotus Redux?", OpinioJuris, 17 June 2012, http://opiniojuris.org/2012/06/17/the-case-of-enrica-lexie-lotus-redux/ accessed 3 October 2015. The Enrica Lexie is an Italian-flagged tanker, with a detachment of six Italian marines on board to deter pirate attacks. On 15 February 2012, two of those marines shot and killed two Indian fisherman on board a fishing boat, the Saint Antony. The facts surrounding the incident are still contested, from the location of the shooting, to the target of the shots, to the circumstances under which the Italian vessel ended up in an Indian port, resulting in the arrest of the two marines. The Italian marines were charged with murder under the Indian Penal Code. The case is now before an arbitral tribunal established under Annex VII of the UN Convention on the Law of the Sea, asked to assert Italian or Indian jurisdiction on the case. For more details on the case, see http://thewire.in/2015/08/10/italy-wants-a-un-tribunal-to-stop-india-from-trying-its-marines-heres-why-its-wrong-8195/ Hollis notes in particular: "what I think does set the case apart from the *Lotus* fact pattern is that the two marines were members of Italy's military. (...) Italian State sovereignty is much more directly at issue in the prosecution of Italian marines who were performing state-mandated functions. (...) the issue is likely to turn on the current state of the international law of sovereign immunity — a key exception to the general rule of territorial prescriptive jurisdiction. In other words, is India legally obligated not to prosecute agents of the Italian state engaged in official governmental actions, *acta jure imperii,* regardless of whether those acts occurred. Or, can India argue that by putting the marines on a private tanker instead of a naval vessel, they should be equated to private security guards instead of agents of the State?

# EXTRATERRITORIAL ENFORCEABILITY OF PRIVACY LAW

An international treaty that regulates jurisdictional claims in data privacy does not exist. There are however, a few authoritative international sources that seem to support extra-territorial data privacy claims.

First and foremost, privacy is included in the Universal Declaration of Human Rights[75], which at Article 12 states; "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"[76]. In addition, the International Covenant on Civil and Political Rights[77] (ICCPR) states in Article 17 that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation". Article 2 obligates the signatories to provide effective legal remedies for any violation of the rights indicated in the Covenant: "Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognised in the present Covenant". Paragraph 3 of the same Article establishes that each State Party undertakes "to ensure that any person whose rights or freedoms as herein recognised are violated shall have an effective remedy". Some scholars claim that, on the basis of this rule in particular, the State signatory of the Covenant is under an obligation "to provide legal protection against unlawful attacks on the privacy of the people subject to its jurisdiction and those present within its territory, regardless of the origins of the attack"[78].

"THE EUROPEAN PRIVACY DIRECTIVE IS THE FIRST AND ONLY INTERNATIONAL DATA-PRIVACY INSTRUMENT TO TACKLE DIRECTLY THE VEXED ISSUE OF WHICH NATIONAL LAW IS APPLICABLE TO A GIVEN CASE OF DATA PROCESSING"

75 United Nations Organization, Universal Declaration of Human Rights, adopted 10 December 1948, http://www.un.org/en/documents/udhr/ accessed 10 October 2015.

76 The Universal Declaration of Human rights was originally not intended as a legally binding document as such but, as its preamble proclaims, "a common standard of achievement for all peoples and nations". See Malcolm Shaw, International Law, 2008, Sixth Edition, Cambridge University Press, 279 "Although clearly not a legally enforceable instrument as such, the question arises as to whether the Declaration has subsequently become binding either by way of custom or general principles of law, or indeed by virtue of interpretation of the UN Charter itself by subsequent practice".

77 United Nations Organization, International Covenant on Civil and Political Rights, entry into force 23 March 1976, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx# accessed 10 October 2015. The ICCPR is part of the International Bill of Human Rights, along with the International Covenant on Economic, Social and Cultural Rights and the Universal Declaration of Human Rights.

78 Dan Svantesson, "The Extraterritoriality of EU Data Privacy Laws – Its Theoretical Justification and Its Practical Effect on U.S. Businesses", 2014, Stanford Journal of International Law, 50 (1), 53-117, 78. See also Dan Svantesson, "The extraterritoriality of EU's Data Privacy Regulation – what does international law say?", March 2014, http://blawblaw.se/2014/03/the-extraterritoriality-of-eu's-data-privacy-regulation-–-what-does-international-law-say/ accessed 9 October 2015: the ICCPR "makes extraterritorial jurisdictional claims mandatory in the data privacy arena".

The Organisation for Economic Co-operation and Development (OECD) Guidelines on Privacy Protection and Transborder Data Flows[79] asserts in paragraph 16 the responsibility of the data controller for the transborder flow of personal data. The rule states that "a data controller remains accountable for personal data under its control without regard to the location of the data."[80] The explanatory memorandum[81] to the OECD Guidelines reveals that the issue of conflict of law was purposely not solved in the final version of the document. The experts only indicated that one way of approaching these problems was to identify one or more connecting factors pointing to one applicable law. It was also suggested that, in a situation where several laws may be applicable, preference be given to the domestic law offering the best protection of personal data[82].

As observed by Lee Bygrave, Directive 95/46 is "the first and only international data-privacy instrument to tackle directly the vexed issue of which national law is applicable to a given case of data processing"[83].

**International sources that seem to support extraterritorial data privacy claims**

1948 - Universal Declaration of Human Rights, Article 12

1976 - International Covenant on Civil and Political Rights
- Article 2 "Each State Party to the present Covenant undertakes to (...) ensure that any person whose rights or freedoms as herein recognized are violated shall have an effective remedy".

2013 - OECD Guidelines on Privacy Protection and Transborder Data Flows
- Paragraph 16 "a data controller remains accountable for personal data under its control without regard to the location of the data."

79 OECD Privacy Framework, 2013, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf accessed 10 october 2015. The Guidelines are an instrument of "soft law": "They are not binding for the OECD Member States, (...) but the OECD has repeatedly and actively tried to make the private sector adopt them as industry guidelines and commit to their principles as well": Myriam Dunn Cavelty, Sai Felicia Krishna-Hensel, Victor Maue "The Resurgence of the State: Trends and Processes in Cyberspace Governance", Ashgate, 2007, 124.

80 This expression replaced the previous "equivalency with domestic legislation", as noted by Lee Bygrave, Data Privacy Law. An International Perspective, Oxford University Press, 2014, 48.

81 The Guidelines, in the form of a Recommendation by the Council of the OECD, were developed by a group of government experts under the chairmanship of The Hon. Mr. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission. The Recommendation was adopted and became applicable on 23 September 1980.

82 Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Article 22, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum accessed 10 October 2015.

83 Lee Bygrave, Data Privacy Law. An International Perspective, Oxford University Press, 2014, 63.

# EXTRATERRITORIAL "TRIGGERS" IN DIRECTIVE 95/46

As regards specifically EU privacy law, the widespread utilization of techniques such as cookies, JavaScript and spyware has determined the processing of an increasing amount of EU data by foreign websites. The European Institutions have addressed these concerns by identifying various situations – "triggers", in the words of Joanne Scott[84] – that allow for the extension of the protection granted by Directive 95/46 to foreign processing.

As seen at the beginning of this Chapter, in international law State jurisdiction can be established through several connecting factors, including the principle of territoriality, the effects theory, the principle of the passive jurisdiction and the principle of nationality.

In the text below, I will analyse which of these were used in EU Directive 95/46 and which appear to have been invoked in the Ruling in order to give rise to the applicability of EU law and the assertion of EU jurisdiction.

## THE PRINCIPLE OF TERRITORIALITY AND TERRITORIAL EXTENSION

A territorial extension happens, according to Joanne Scott, when triggers are identified that justify the application of EU law upon non-EU subjects and in relation to conduct that takes place outside of the territory. The meaning of territory in EU law was clarified by the CJEU in the case known as Air Transport Association of America, where the relevant Directive 2008/101 was deemed applicable to aircraft engaged in international navigation when they "enter or depart from the territory of the Member States" [85].

In Directive 95/46, the territoriality principle and the trigger for territorial extension are engrained in Article 4, 1 (a)[86], where the applicability of EU law is connected to the location of the data processing.

According to Lokke Moerel, the nature of the territoriality principle found in Article 4, 1 (a) is "more or less virtual"[87]: the law abstracts from both the location of the data controller and that of the performance of the data-processing activity, but adheres to the territoriality principle when it establishes a virtual connection with the EU territory. This is accomplished when the Article refers to an establishment of the foreign data controller on the territory of a Member State as a condition for the applicability of EU law. Furthermore, it is not required that the data processing be performed within that establishment, but rather "in the context" of its activity. Interestingly, the study of the legislative history that resulted in Directive 95/46 reveals that both the Original Proposal (COM (1990) 314–2, 1990/0287/COD) and the Amended Proposal (COM

84 "Trigger is a mechanism that launches the application of EU law and delimits its personal and territorial scope of application", Joanne Scott, "The new EU Extraterritoriality", Common Market Law Review, Vol. 51 No. 5 October 2014, 1343-1380, 1344, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2464240 accessed 9 October 2015.

85 CJEU, C-366/10, Air Transport Association of America (ATAA) & Others v. Secretary of State for Energy and Climate Change, ECLI:EU:C:2011:864, paragraph 131 http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=366/10&td=ALL accessed 9 October 2015

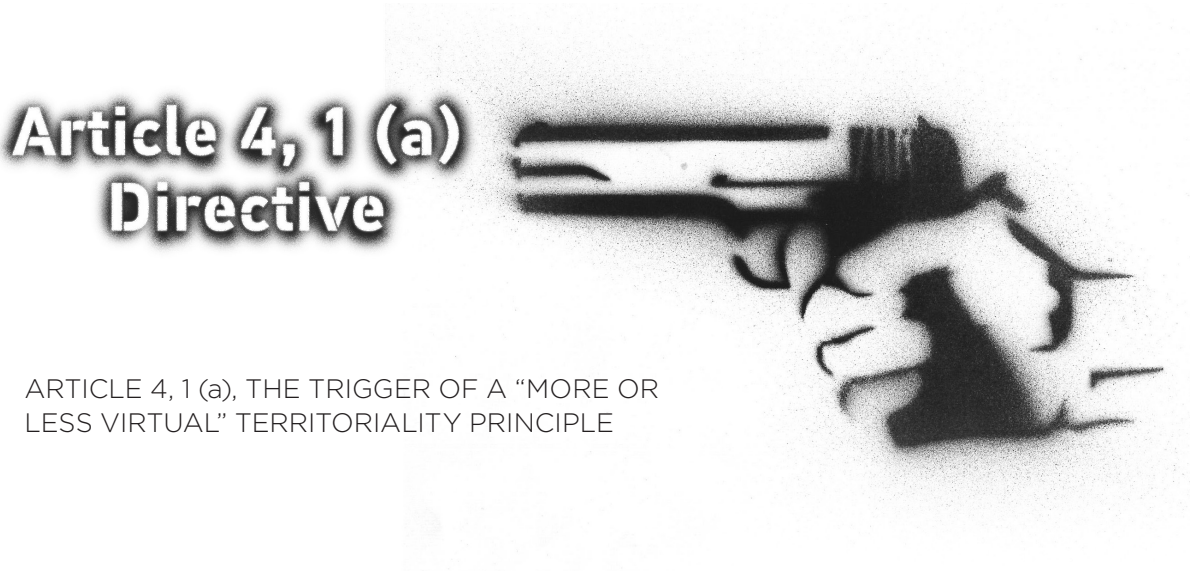
86 See *supra,* note 13.

87 Lokke Moerel, "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", International Data Privacy Law, 2011, Vol. 1, No 1, 29, http://idpl.oxfordjournals.org/content/early/2010/11/02/idpl.ipq004, accessed 9 October 2015.

(92) 422 final–SYN 287) incorporated different nuances of the country-of-origin principle. The connecting factor was respectively identified in the location of the data and in the establishment of the controller within a Member State.

With the final formulation of Article 4, 1 (a), the EU legislator targeted the case that emerged in the discussions around the proposals, of servers being placed in countries with particularly benign data-protection laws: with the reference to the "place of establishment" and the "context of activity" it was ensured that such an *escamotage,* or dodge, would not void the protection provided by the Directive[88].

In 2008, the Article 29 Working Party published an Opinion on Search Engines[89] aimed at giving guidance in the interpretation of Article 4, 1 (a). The document specifically refers to the case of the establishment of a foreign search engine, which "is involved in the selling of targeted advertisements to the inhabitants of that state" as satisfying the condition of "processing in the context of the activity of the establishment". It is easy to recognise here both the concept and wording used six years later by the CJEU in the Ruling, when at paragraph 57 it established the applicability of Spanish data privacy law to the search activity performed by Google Inc. on grounds of the inextricable link with Google Spain.




ARTICLE 4, 1 (a), THE TRIGGER OF A "MORE OR LESS VIRTUAL" TERRITORIALITY PRINCIPLE

The reasoning is the same followed by the Supreme Court of British Columbia in Equustek, when it found for its territorial jurisdiction over Google Inc. with an argument based on contextual advertising[90].

In both these cases, we can observe that the trigger contained in the law was used to establish jurisdiction on a foreign subject who performs an activity entirely abroad, on the basis of the EU Member State nationality held by their subsidiaries: an extraterritorial extension of competence defined as a "subsidiary jurisdiction" by Joanne Scott[91].

88 For a thorough analysis of the legislative history of Directive 95/46 see Lokke Moerel, "Back to basics: when does EU data protection law apply?", International Data Privacy, 2011, 3-7, http://idpl.oxfordjournals.org/content/early/2011/01/24/idpl.ipq009.full.pdf+html accessed 11 October 2015.

89 Article 29 Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines" (WP 148, 4 April 2008), 10, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf accessed 9 October 2015.

90 See Equustek, paragraph 63 and *supra,* 2.4 "Implementation of the Ruling by judicial authorities: Canada, the Equustek case".

91 Scott, "The new EU Extraterritoriality", 1352.

# THE EFFECTS THEORY

The recourse of the CJEU to the effects theory[92] is strongly suggested by the language of the decision in Costeja. The preoccupation over the impact that the global reach of Google Search may have on factually voiding the protection ensured by Directive 95/46 recurs throughout the Ruling. Whenever applying a broad interpretation to the letter of the law, the Court indeed repeats that this seems necessary in order to ensure a "effective and complete protection" of the data subjects[93]. The most unequivocal reference to the effects theory is found in Paragraph 58 of the Ruling, where the Court declares: "it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure".

# PASSIVE PERSONALITY PRINCIPLE AND NATIONALITY PRINCIPLE

The language used by the CJEU in the Ruling that made us recognise the application of the effects theory, could suggest also the recourse to the passive personality principle, according to which States can claim jurisdiction over offences committed abroad by foreigners when these affect its citizens. However, nowhere in the Directive can be found reference to the nationality, or even the domicile, of the protected data subject[94].

The Directive approaches the right to privacy from the point of view of human rights, irrespective of nationality. As a consequence, for EU privacy law to apply it is unnecessary that the data being processed pertain to a EU citizen, or that the data subject resides in the Union. This circumstance could potentially bring the concept of "law shopping" to an entirely new level, as an Australian national could, for example, sue search engines before the Court of a Member State to obtain global de-linking of results from a web search on the basis of his name, on the grounds that the engine has an establishment in that State.

It should be noted that the passive personality principle and the nationality principle are at present part of the proposed EU General Data Protection Regulation, expected to be approved by the end of 2015. The geographical scope of application of the Regulation is delineated in Article 3, which maintains the reference to the processing of data being performed in the context of the activity of an establishment in a Member State, but also indicates as a criterion for application the residence of the data subject in the Union[95].

---

92 For a investigation on the dangers of applying the effects theory to the Internet, see Jonathan Zittrain, "Be Careful What You Ask For: Reconciling a Global Internet and Local Law" Harvard Law School Public Law, 2003, Research Paper No. 2003-03 5/2003, 5 http://cyber.law.harvard.edu/wg_home/uploads/204/2003-03.pdf accessed 11 October 2015.

93 See for example CJEU, Case C-131/12, paragraphs : 34, 53, 84.

94 Preamble of Directive 95/46, Article 2: "data-processing systems (...) must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy". In Article 2, "Definitions", where the law identifies the meanings of "data subject" and "personal data", no reference to nationality.

95 Council of the European Union, "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 15 June 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf accessed 11 October 2015. Article 3: *Territorial scope:* 1.This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union. 2. This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment by the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the European Union. 3. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

# CONCLUSION


The CJEU decision on the Costeja and Google case had the merit of sparking a global debate on a subject – privacy – that is often dismissed as plain boring, or which is generally overlooked as a fundamental human right by a large part of the general public. It was interesting to observe the evolution of the opinions in the 18 months since the Ruling. Some of the scholars, journalists and civil-society advocates who originally reacted with outrage to a decision mainly perceived as an attempt at censorship, are now shifting towards positions that take into consideration the possibly acceptable reasons why a person could wish to "unlink" their name from specific information.

Personally, I struggle to find any other straightforward positive consequence of the decision.

It feels like the Court took a shortcut in adapting privacy rules conceived in the 1990s to the reality of today's overwhelmingly virtual life. In particular, the text of the Ruling seems to lack any attempt at clarity, or forward thinking, as if the decision was taken with a focus on the specificities of the case before the Court, and with little concern for its implications. When invested with the opportunity to rule on a case that quite evidently closely tackled the role of the Internet in people's lives, the judges could, in my opinion, have applied their legal skills in a more comprehensive way, embracing the fact that they were creating a precedent for the future reference of legislators, judicial authorities and civil society. The Court decided instead to keep their wording as vague as possible, mitigating with equally obscure exceptions any strong, definitive statement.

One conspicuous example is paragraph 81 of the decision: "Whilst it is true that the data subject's rights protected by those Articles also override, as a general rule, the interest of Internet users, that balance may however depend, in specific cases, on the nature of the information in

question and its sensitivity for the data subject's private life and on the interest of the public in having that information, an interest which may vary, in particular, according to the role played by the data subject in public life." The number of questions that such a cautious declaration raises is incalculable. First and foremost, who decides what the balance is? What are the "specific cases" to which the exceptions apply, and who specifies them? What kind of information has a nature that makes it worthy of remaining available to the public? What aspects of the data subjects' private life are concerned by information that is "sensitive"? In which territory must the data subject play a role for this circumstance to be relevant, must it be at least national? Should the public role be a present reality, or is a public figure of the past still considered the subject of prevailing interest from the public? How much time is enough to consider the information no longer relevant? If the public role is just explanatory of a situation worthy of exception, then what are the others?

The list of questions could continue, and it is mirrored by the fierce debate that the Ruling sparked and that does not appear to be fading. The point is that by taking this road, the Court abdicated from the position of rule maker. Search engines and Data Privacy Authorities were left to autonomously establish what their behaviour should be in the aftermath, a task that they performed while limiting mutual consultations to the minimum, and thus ending up with positions that are largely incompatible.

The debate that originated from the lack of rules in the CJEU decision has been mainly focused on its extraterritorial implications, but the absence of clear direction is evident in more than one aspect of the implementation of the Ruling.

In a situation where their obligations were far from defined, rather than running the risk of facing costly transactions in judicial proceedings, Google decided to take a proactive approach and engage directly in the evaluation of the de-linking requests. It implemented a system that is very similar to the one reserved to claims of copyright infringement, with a "notice and take-down" approach, on the basis of rules and parameters that Google for the most part invented. The original sin is that, while in the case of copyright[96] the process is clearly prescribed in a law, complete with obligations and consequences for all subjects involved, in the case of privacy, the de-linking procedure is largely an instrument of self-discipline.

For their part, Data Protection Authorities and the Article 29 Working Party produced rules of their own liking, a redundant effort due to their inability to issue binding directions upon search engines.

The guarded approach adopted by the Court resulted in a situation where the matter of de-indexing for privacy reasons is now handled in a state of anarchy, at the centre of a genuine battlefield between search engines and Data Protection Authorities, a bickering war that is not likely to bring solutions any time soon to either the protection of data subjects, or the certainty of the law.

96 In cases of claims of copyright infringement, Google applies the United States Digital Millennium Copyright Act (DMCA) of 1998, which establishes at section 512(c)(3) the details for the notice and takedown procedure. The copyright owner submits the requests under penalty of perjury, and the lack of reaction from the Service Provider engages its monetary liability. The DMCA also establishes a form of defence for the original publisher, which is notified of the procedure and can file a counter notification. Incurring in misrepresentation results in damages liability for all the subjects involved: the alleged infringer, the copyright owner or its licensee, or the service provider.

On 6 October 2015, the CJEU decided another case[97] destined to represent a landmark in matters of privacy, when it invalidated the Safe Harbour agreement, which brought the transfer of data from the EU to the United States within the provisions of Directive 95/46. The result of the Ruling is that presently the United States does not ensure an adequate level of protection of private data for the purposes of Article 25, 1[98] of the Directive.

In this scenario, the Privacy Regulation that the European Union plans to approve by the end of 2015 is invested with a relevance that the legislator cannot ignore.

The European Union finds itself in the position of main advocate for the human right of privacy in the global landscape, and this is the perspective that the Regulation needs to embrace. The legislator should rise above the limits of Directive 95/46 and realise, for example, that maintaining the criteria of the establishment on the EU territory as a trigger for the application of EU privacy law is probably inadequate to the global nature of the Internet. Moreover, this potentially creates an unjust competitive advantage in favour of search engines that do not have a territorial link with a Member State, but that nevertheless undoubtedly process EU data.

**TOWARDS A FRAMEWORK ON PRIVACY PROTECTION UNDER GENERAL PRINCIPLES OF INTERNATIONAL LAW**

**Possible sources:**

International obligations from Treaties

Negotiations in trade agreements

General principles on the basis of decisions of International Bodies like
- International Court of Justice
- The International Tribunal for the Law of the Sea
- International Criminal Court/ad hoc Criminal Tribunals

Or regional
- Inter-American Court of Human Rights/European Court of Human Rights

Essentially, the European Union has the opportunity to build on the experience of the uncertainty created by the latest CJEU decisions and directly address the very specific case of the processing of data through the Internet in the new millennium.

It has become apparent that the Courts, the privacy authorities and organisations around the world need guidance and positive privacy rules by which to abide. Those rules are likely to originate from multiple sources. The European Privacy Regulation has the potential to be one of those, if it will take into consideration the reality of the global Internet rather than limiting its scope to the imposition of regional laws upon foreign operators. It seems to me that the US Digital Millennium Act could serve as inspiration for a EU law that has the potential to be accepted and applied beyond EU borders.

97 CJEU Case C-362/14, Schrems v. Data Protection Commissioner, http://static.ow.ly/docs/schrems_3OHQ.pdf accessed 10 October 2015. Pursuant to the refusal of the Commissioner to investigate Mr. Schrems' complaint regarding the fact that Facebook Ireland Ltd transfers and stores users personal data in the United States of America, the Irish High Court referred the case to the CJEU for a preliminary ruling that assessed the validity of Commission Decision 2000/520 in relation with the Charter of Fundamental Rights of the European Union and Directive 95/46. The Commission decision set out in its Annex I the "Safe Harbour Principles" which, implemented in accordance with the guidance provided by the frequently asked questions ("the FAQs") issued by the US Department of Commerce on 21 July 2000 and collected in Annex II of the same decision, ensured an adequate level of protection for personal data transferred from the Community to organisations established in the United States, in accordance with the provisions of Article 25 of Directive 95/46. The Commission decision is accessible online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML. Mr. Schrems asked the Commissioner to prohibit Facebook Ireland from transferring his personal data to the United States, contending that "the law and practice in force in that country did not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by the public authorities" (paragraph 25 of the CJEU decision). The CJEU found that decision 2000/520 of the Commission was invalid.

98 Directive 95/46, Article 25: "Principle 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection."

**THE CHALLENGE**

The European Union is now the main advocate for the human right of privacy in the global landscape

**EU COULD**

Make the DP Regulation the starting point of a process that brings protection of privacy into the new millennium

**CJEU MIGHT**

Rise above an exclusively Eurocentric perspective and contribute to the creation of general principles of International Law on privacy matters

In addition, new agreements need to be negotiated in order to find acceptable solutions tailored to the challenges to privacy represented by the rules in place in countries where European data are actually processed.

It seems likely that privacy will become a factor in the negotiations of trade agreements in other regions of the world, as happened with intellectual property at the time of the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement in 1994.

All these sources will hopefully constitute a framework on privacy protection under general principles of International Law, built also on the basis of the decisions of International Courts[99] that could provide principles applicable in privacy matters. Such courts include the International Court of Justice, the International Tribunal for the Law of the Sea, possibly the International Criminal Court and the ad hoc Criminal Tribunals established by the United Nations, but also regionally based courts such as the Inter-American Court of Human Rights and the European Court of Human Rights. In this process, a role will likely be played by bodies such as the Human Rights Committee, the group of independent experts that monitors implementation of the International Covenant on Civil and Political Rights[100] by its State parties.

The Court of Justice of the European Union has the possibility to be part of this chain of events and contribute to the creation of an international framework around the protection of privacy, provided that it succeeds in adopting a less exclusively Eurocentric perspective, and instead seizes the opportunity to create viable global precedents. If it succeeds, the Anglo-Saxon press may finally treat the CJEU with the respect it deserves, rather than persistently referring to it as "a European Court"[101].

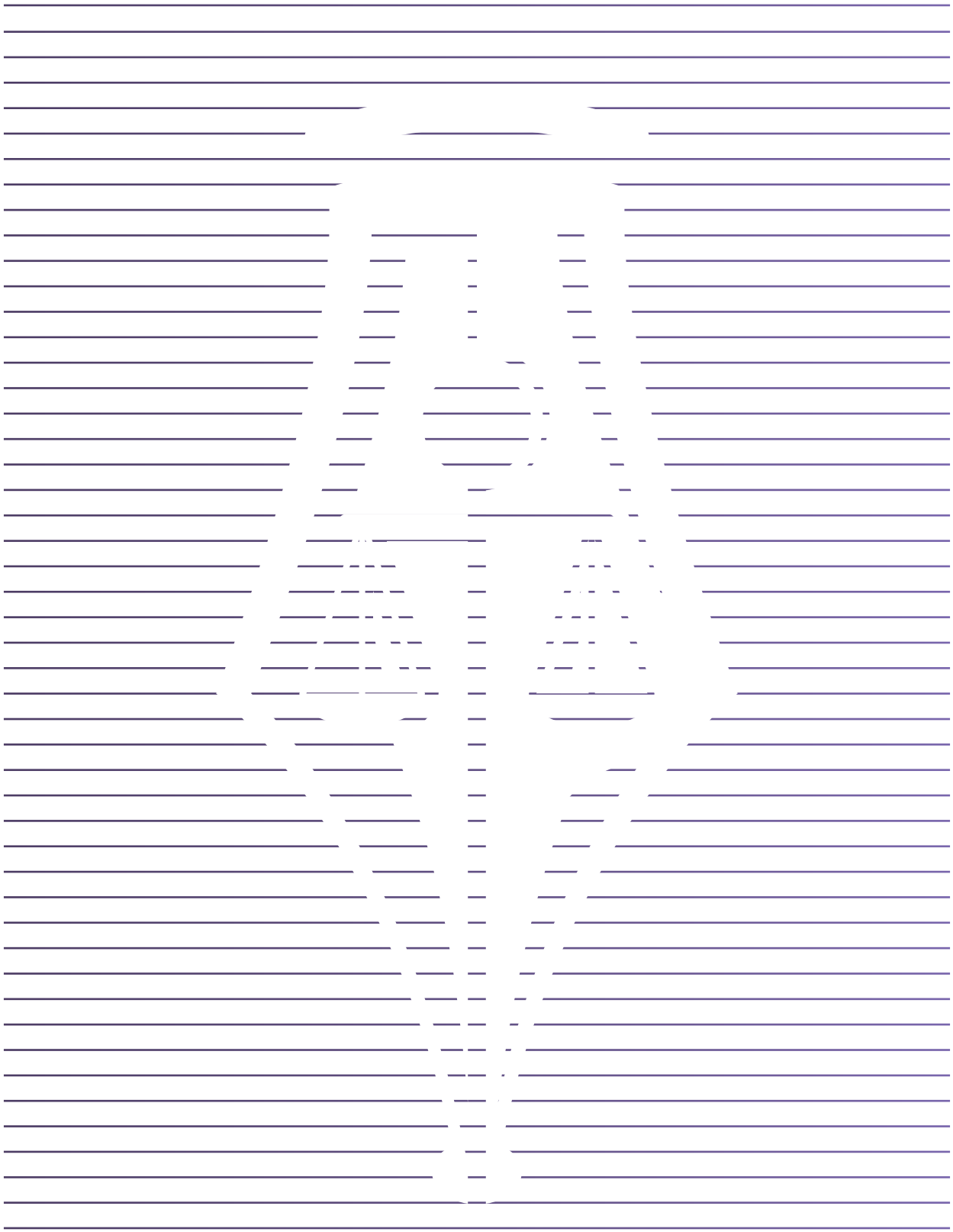
Paris, 20 October 2015

99 The ruling on the Enrica Lexie case, for example, will likely help define the limits of extraterritorial jurisdiction, see *supra,* note 76.

100 See *supra,* note 79.

101 One of many examples here, from Newsweek reporting on the Schrems case: http://www.newsweek.com/why-has-european-court-banned-sending-personal-data-across-atlantic-381377

# BIBLIOGRAPHY



# STATUTES, REGULATIONS, DIRECTIVES AND TREATIES:

**British Columbia,** Statutes and Regulations, Court Jurisdiction And Proceedings Transfer Act [Sbc 2003] Chapter 28, http://www.canlii.org/en/bc/laws/stat/sbc-2003-c-28/latest/sbc-2003-c-28.html

**European Union:** 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, Official Journal L 281 , 23/11/1995 P. 0031 – 0050, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

**European Union:** Charter Of Fundamental Rights Of The European Union, (2000/C 364/01), entry into force 1 December 2009, http://www.europarl.europa.eu/charter/pdf/text_en.pdf

**European Union,** Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX-:32000D0520:EN:HTML

**International Court of Justice,** Statute http://www.icj-cij.org/documents/index.php?p1=4&p2=2&p3=0

**Spain: Organic Law No 15/1999** of 13 December 1999 on the protection of personal data (BOE No 298 of 14 December 1999, p. 43088), transposing into Spanish Law Directive 95/46.

**United Nations Organization,** Universal Declaration of Human Rights, adopted 10 December 1948, http://www.un.org/en/documents/udhr/

**United Nations Organization,** International Covenant on Civil and Political Rights, entry into force 23 March 1976, http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx#

# CASE LAW:

**British Columbia,** Thumbnail Creative Group Inc. v. Blu Concept Inc., 2009 BCSC 1833 (CanLII), http://www.courts.gov.bc.ca/jdb-txt/SC/09/18/2009BCSC1833.htm

**British Columbia,** Supreme Court, Equustek Solutions Inc. v. Jack, 2014 BCSC 1063 (CanLII), http://www.canlii.org/en/bc/bcsc/doc/2014/2014bcsc1063/2014bcsc1063.html

**British Columbia,** Supreme Court, Niemela v. Malamas, 2015 BCSC 1024 (CanLII) http://canlii.ca/t/gjk4w

**Canada,** Club Resorts Ltd. v. Van Breda, [2012] 1 SCR 572, 2012 SCC 17 (CanLII), http://www.canlii.org/en/ca/scc/doc/2012/2012scc17/2012scc17.html

**Council of the European Union,** "Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)", 15 June 2015, http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf

**European Union,** CJEU, Case C-73/07 Satakunnan Markkinapörssi and Satamedia ECLI:EU:C:2008:727, http://curia.europa.eu/juris/liste.jsf?language=en&num=C-73/07

**European Union,** CJEU, C-366/10, Air Transport Association of America (ATAA) & Others v. Secretary of State for Energy and Climate Change, ECLI:EU:C:2011:864, http://curia.europa.eu/juris/liste.jsf?language=en&jur=C,T,F&num=366/10&td=ALL

**European Union,** CJEU, Case C-131/12 Google Spain and Google Inc v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González, ECLI:EU:C:2014:317, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62012CJ0131

**European Union,** CJEU Case C-362/14, Schrems v. Data Protection Commissioner, http://static.ow.ly/docs/schrems_3OHQ.pdf

**France,** Tribunal de Grande Instance de Paris, Ord. de réf., 16 September 2014, M. et Mme X et M. Y / Google France, http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4291 **France,** Tribunal de Grande Instance de Paris, Ord. de réf., 19 December 2014, Marie-France M. / Google France et Google Inc. http://junon.univ-cezanne.fr/u3iredic/?p=16671

**International Court of Justice,** North Sea Continental Shelf Cases, 20 February 1969, http://www.icj-cij.org/docket/files/51/5535.pdf

**International Court of Justice,** Accordance with International Law of the Unilateral Declaration of Independence in Respect of Kosovo, Advisory Opinion, I.C.J. Reports 2010, p. 403, http://www.icj-cij.org/docket/files/141/15987.pdf

**Organisation For Economic Co-Operation And Development OECD,** Explanatory Memorandum to the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum

**Organisation For Economic Co-Operation And Development OECD,** Privacy Framework, 2013 http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

**Permanent Court of International Justice,** S.S. "Lotus" (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (7 September) http://documents.law.yale.edu/sites/default/files/SS%20Lotus%20-%20PCIJ%20-%201927.pdf

**United Kingdom,** Data Protection Act 1998 Supervisory Powers of the Information Commissioner Enforcement Notice dated 18 August 2015, https://ico.org.uk/media/action-weve-taken/enforcement-notices/1432380/google-inc-enforcement-notice-18082015.pdf

**United States,** Zippo Manufacturing v. Zippo Dot Com Inc., 952 F. Supp. 119 (W.D. Pa. 1997) http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm

# SOURCES


**Advisory Committee to Google on the Right to be Forgotten,** Report, 22 February 2015, http://www.cil.cnrs.fr/CIL/IMG/pdf/droit_oubli_google.pdf

**Article 29** Data Protection Working Party, "Opinion 1/2008 on data protection issues related to search engines" (WP 148, 4 April 2008), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2008/wp148_en.pdf

**Article 29** Data Protection Working Party, "Guidelines On The Implementation Of The Court Of Justice Of The European Union Judgment On "Google Spain And Inc V. Agencia Española De Protección De Datos (Aepd) And Mario Costeja González" C-131/12", http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf

**James Ball,** "'Right to be forgotten' ruling creates a quagmire for Google et al", The Guardian, 13 May 2014, http://www.theguardian.com/commentisfree/2014/may/13/right-to-be-forgotten-ruling-quagmire-google

**Lee Bygrave,** Data Privacy Law. An International Perspective, Oxford University Press, 2014

**Antonio Cassese,** "International Law", Oxford University Press; 2 edition, 10 February 2005

**Myriam Dunn Cavelty, Sai Felicia Krishna-Hensel, Victor Maue** "The Resurgence of the State: Trends and Processes in Cyberspace Governance", Ashgate, 2007

**Commission nationale de l'informatique et des libertés,** "CNIL orders Google to apply delisting on all domain names of the search engine", 12 June 2015, http://www.cnil.fr/english/news-and-events/news/article/cnil-orders-google-to-apply-delisting-on-all-domain-names-of-the-search-engine/

**Commission nationale de l'informatique et des libertés,** "Right to delisting: Google informal appeal rejected", 21 September 2015, http://www.cnil.fr/english/news-and-events/news/article/right-to-delisting-google-informal-appeal-rejected/

**Peter Fleischer,** "Response to the Questionnaire addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the "right to be forgotten"", 31 July 2014, https://docs.google.com/file/d/0B8syaai6SSfiToEwRUFyOENqR3M/edit?pli=1

**Peter Fleischer,** "Implementing a European, not global, right to be forgotten", 30 July 2015, http://googlepolicyeurope.blogspot.fr/2015/07/implementing-european-not-global-right.html

**Google Transparency Report** https://www.google.com/transparencyreport/removals/europeprivacy/?hl=en

**Duncan Hollis,** "The Case of Enrica Lexie: Lotus Redux?", Opinio Juris, 17 June 2012, http://opiniojuris.org/2012/06/17/the-case-of-enrica-lexie-lotus-redux/ accessed 3 October 2015.

**Uta Kohl,** Jurisdiction and the Internet – Regulatory Competence of Online Activity, (Cambridge University Press 2007)

**David Lee,** "Google ruling 'astonishing', says Wikipedia founder Wales", BBC News Technology, BBC News Technology, 14 May 2014, http://www.bbc.com/news/technology-27407017

**Arthur Lenhoff,** "International Law and Rules on International Jurisdiction", Cornell Law Review, Vol. 50, Fall 1964, http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2435&context=clr

**Lokke Moerel,** "The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?", International Data Privacy Law, 2011, Vol. 1, No 1, http://idpl.oxfordjournals.org/content/early/2010/11/02/idpl.ipq004

**Lokke Moerel,** "Back to basics: when does EU data protection law apply?", International Data Privacy, 2011, http://idpl.oxfordjournals.org/content/early/2011/01/24/idpl.ipq009.full.pdf+html

**Robert Peston,** "Why has Google cast me into oblivion?", BBC News Business, 2 July 2014 http://www.bbc.com/news/business-28130581

**Joanne Scott,** "The new EU Extraterritoriality", Common Market Law Review, Vol. 51 No. 5 October 2014, 1343-1380, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2464240

**Vera Shaftan,** "Russia signs controversial 'right to be forgotten' bill into law", http://www.dataprotectionreport.com/2015/07/russia-signs-controversial-right-to-be-forgotten-bill-into-law/

**Malcolm Shaw,** International Law, 2008, Sixth Edition, Cambridge University Press, https://www.academia.edu/3386070/Malcolm_N._Shaw_-_International_Law_6th_edition_2008

**Dan E. Stigall,** "International Law and Limitations on the Exercise of Extraterritorial Jurisdiction in U.S. Domestic Law", Hastings International and Comparative Law Review, Vol. 35, No. 2, p. 323, 2012, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2043287

**Dan Svantesson,** "The Extraterritoriality of EU Data Privacy Laws – Its Theoretical Justification and Its Practical Effect on U.S. Businesses", 2014, Stanford Journal of International Law, 50 (1), 53-117.

**Dan Svantesson,** "The extraterritoriality of EU's Data Privacy Regulation – what does international law say?", March 2014, http://blawblaw.se/2014/03/the-extraterritoriality-of-eu's-data-privacy-regulation-–-what-does-international-law-say/

**Sylvia Tippmann and Julia Powels,** "Google accidentally reveals data on 'right to be forgotten' requests", The Guardian, 14 July 2015, http://www.theguardian.com/technology/2015/jul/14/google-accidentally-reveals-right-to-be-forgotten-requests

**Jonathan Zittrain,** "Be Careful What You Ask For: Reconciling a Global Internet and Local Law" Harvard Law School Public Law, 2003, Research Paper No. 2003-03 5/2003, http://cyber.law.harvard.edu/wg_home/uploads/204/2003-03.pdf

Public Affairs
Media Policy

**21st March 2016**



**www.wan-ifra.org/policy**