

**IN THE COURT OF JUSTICE OF THE EUROPEAN UNION**

**Case C-507/17**

**GOOGLE INC.**

**Applicant**

**V**

**COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTES  
(CNIL)**

**Defendant**

---

**WRITTEN OBSERVATIONS OF IRELAND**

---

Dated this 7<sup>th</sup> day of December 2017

To the President and Members of the Court of Justice of the European Union

Pursuant to Article 23 of the Protocol on the Statute of the Court of Justice of the European Union, Ireland, represented by Maria Browne, Chief State Solicitor, Osmond House, Little Ship Street, Dublin 8, acting as agent, accepting service via e-curia, with an address for service at the Embassy of Ireland, 28 route d'Arlon, Luxembourg, assisted by Miss Margaret Gray, Barrister-at-Law, of the Bar of Ireland, has the honour of submitting these written observations.

1. This reference for a preliminary ruling under Article 267 of the Treaty on the Functioning of the European Union (“TFEU”) was made on 19 July 2017 (lodged on 21 August 2017) by the Conseil d’État of the French Republic (“the Referring Court”). The referred questions concern the territorial scope of certain provisions of Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281 p.31) (“the Directive”).

## THE ORDER FOR REFERENCE

2. Ireland refers to the facts as described in the Order for Reference. In brief outline, on 21 May 2015, CNIL served notice on Google Inc that when acceding to a request for delisting it must remove the requested item from search results made using any of its domain names. On 10 March 2016, the CNIL Select Panel found that Google had failed to comply within the time-limit and imposed a penalty of €100,000. Google is seeking to have that ruling quashed.

### *The legal framework as outlined by the Conseil d’État*

3. The Referring Court considered the position that certain provisions of French law define “processing of personal data” and a “controller”, thus transposing Article 2(b) and (d) of the Directive. Relevantly, in Case C-131/12 **Google Spain SL v AEPD**,<sup>1</sup> the CJEU held that search engine activity is classified as processing of personal data within the meaning of Article 2(b) and the operator of a search engine is a controller within the meaning of Article 2(d).
4. Further, French law states that it will only apply in French territory, thus transposing Article 4(1)(a) of the Directive. Related to that principle, in **Google Spain**, the CJEU held that processing of personal data is carried out in the territory of a Member State if the operator of a search engine sets up a branch or subsidiary in the Member State intended to promote and sell advertising space and orientating its activity towards the inhabitants of that Member State.

---

<sup>1</sup> Case C-131/12 **Google Spain SL v AEPD** ECLI:EU:C:2014:317

5. Therefore, the Referring Court recounted that the processing of personal data by the search engine operated by Google Inc, when taking into account the promotion and selling of advertising space by Google France, comes within the scope of French law.

*The existence of a right to de-referencing*

6. The Referring Court also noted that French law provides the right to object on legitimate grounds if proof of identity is provided, thus transposing Article 14(a) and Article 12(b) of the Directive. Again, in **Google Spain**, the CJEU held that these provisions had the effect that a search engine operator is obliged to remove from search results made on the basis of a person's name links to web pages even when the publication of the information is lawful and is not required to be removed from the web page itself. Therefore, a search engine operator carrying out data processing in France must grant requests for de-referencing.

*The competence and scope of the powers of the CNIL Select Panel*

7. The Referring Court considered that French law provides that if the data processing controller fails to fulfil its obligations then CNIL can serve notice to bring the infringement to an end within the period specified. If there is no compliance, then the CNIL Select Panel will hear both parties and can impose penalties. This appears to transpose Article 24 of the Directive, which places sanctions within the remit of Member States.
8. Therefore, the Referring Court considered that the CNIL Select Panel is competent to hear and adjudicate upon the dispute, provided that the controller's activity is within France, even if only partially within France.

*The classification of a search engine as single act of processing personal data*

9. The Referring Court noted that the act of processing may constitute a set of operations – in this case, indexing web content and making it available to internet users in a given order of preference – but that this does not prevent it from being regarded as single act of processing personal data. In this case, search engine operated by Google Inc are made up of various domain names distinguished by

geographical extensions in order to display results adapted to specific cultural (not least linguistic) characteristics of that territory.

10. The Referring Court noted that a search conducted from google.com is, in principle, automatically redirected to an applicable domain based on the user's location as determined by IP address. Whatever the user's location, he can conduct searches using any of the domain names. Although results may differ depending on the domain used, it is common ground that the links displayed come from common databases and common indexing.
11. All Google domain names can be accessed from French territory, there are gateways between the domains (e.g. the automatic redirection from google.com), and there are cookies present on extensions other than the one on which they were first placed. Therefore, this search engine (which has been subject of only one declaration to CNIL) can be classified as a single act of processing personal data
12. On the facts, the processing was within French territory, and, therefore, CNIL was competent to impose a financial penalty as it had not mischaracterised the activity of Google's search engine as a single act of data processing.

*The scope of the right to de-referencing*

13. CNIL, thus, penalised Google as it refused to apply de-referencing to all of its domain names, applying it only to those corresponding to EU Member States.
14. CNIL regarded as insufficient Google's further proposal as to geo-blocking (which was, in any event, made after the time-limit in the formal notice had passed), whereby users would be blocked if using an IP address in the Member State where the subject of the de-referencing resides.
15. Google argued that the provisions of the Directive as interpreted by the CJEU do not mean that the links should be removed from searches on all of its domain names and that this breaches public international law principles of comity and non-interference. Google also argued that it is a disproportionate interference with the rights to freedom of expression, information, communication and the press.

16. Considering that the determination of the dispute before it raised serious issues of EU law, the Referring Court posed the following questions to the CJEU:

*“1. Must the ‘right to de-referencing’, as established by the Court of Justice of the European Union in its judgment of 13 May 2014 on the basis of the provisions of Articles 12(b) and 14(a) of Directive [95/46/EC] of 24 October 1995, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated on the basis of the requester’s name is conducted, and even if it is conducted from a place outside the territorial scope of Directive [95/46/EC] of 24 October 1995?”*

*2. In the event that Question 1 is answered in the negative, must the ‘right to de-referencing’, as established by the Court of Justice of the European Union in the judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, only to remove the links at issue from the results displayed following a search conducted on the basis of the requester’s name on the domain name corresponding to the State in which the request is deemed to have been made or, more generally, on the domain names distinguished by the national extensions used by that search engine for all of the Member States of the European Union?”*

*3. Moreover, in addition to the obligation mentioned in Question 2, must the ‘right to de-referencing’, as established by the Court of Justice of the European Union in its judgment cited above, be interpreted as meaning that a search engine operator is required, when granting a request for de-referencing, to remove the results at issue, by using the ‘geo-blocking’ technique, from searches conducted on the basis of the requester’s name from an IP address deemed to be located in the State of residence of the person benefiting from the ‘right to de-referencing’, or even, more generally, from an IP address deemed to be located in one of the Member States subject to Directive [95/46/EC] of 24 October 1995, regardless of the domain name used by the internet user conducting the search?”*

### **OBSERVATIONAL POINTS IN COMMON TO THE THREE QUESTIONS**

17. Before addressing the questions posed by the Referring Court, and Ireland’s responses to those questions, it is necessary, in the first instance, to consider certain provisions in the Directive.

18. Article 4 provides that national law shall be applicable, and, as a primary rule, within the territory of the Member States, as follows:

*“1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:*

*(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;*

*(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;*

*...”*

19. To recall, Article 6 of the Directive establishes the principles that apply to Member States in relation to data quality. Member States and, in turn, controllers of data processing, are obliged to adhere to the principles set out in Article 6, as confirmed by this Court in **Google Spain** (at paragraph 72). Expressly, Article 6(1)(b) requires Member States to provide that personal data must be *“collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”*.

20. Article 7 of the Directive sets the criteria according to which data processing may be legitimate (save for special categories of data, which are dealt with in Article 8). Article 7(f) permits processing where *“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 [or] fundamental rights and freedoms of the data subject which require protection under Article 1(1).”* In that regard, consideration of whether or not Article 7(f) provides a basis for the justification of lawful processing of personal data may, in some instances, require the balancing of competing interests, being those of other interested parties against those rights of the data subject.

21. Article 8 provides for the processing of special categories of personal data, and, Article 8(1) lays down the following prohibition:

*“Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.”*

22. Article 8(3) and (4) lay down certain grounds for derogating from the prohibition in Article 8(1). Article 8(5) provides as follows:

*“5. Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law, subject to derogations which may be granted by the Member State under national provisions providing suitable specific safeguards. However, a complete register of criminal convictions may be kept only under the control of official authority.”*

23. Article 9 seeks to reconcile processing of personal data, on the one hand, and freedom of expression on the other.

24. Article 12 deals with a data subject’s right of access to data and certain remedies including, under Article 12(b), the right to obtain from the controller *“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 incompatible or inaccurate nature of the data”*.

25. Article 14, which is entitled “The data subject’s right to object”, provides:

*“Member States shall grant the data subject the right:*

*(a) at least in the cases referred to in Article 7(e) and (f), to object at any time on compelling legitimate grounds relating to his particular situation to the processing of data relating to him, save where otherwise provided by national legislation. Where there is a justified objection, the processing instigated by the controller may no longer involve those data...”*

26. The three questions referred each have as their locus the territorial scope of application of the de-listing obligation in the Directive.
27. It is established, and was recently confirmed by the Commission in its Factsheet on the ruling in *Google Spain* and the “right to be forgotten”, that this is not a “super right” and, necessarily, must be balanced against other rights. This assessment as to both the content of rights and the balancing exercise, falls, in the first instance, to the controller. The precise contours and outcome of assessment will potentially vary as between Member State and Member State and, certainly, as between Member States and third countries.
28. It is clear that a Member State and parties subject to the rights and obligations arising under the Directive may exercise discretion in carrying out balancing of rights exercises in relation to a number of issues arising under the Directive. This includes when Member States and parties are required to determine the scope of protection for data subjects when certain grounds for derogating or limiting the prohibition in Article 8(1) present themselves, and when they are required to determine the scope of the right to obtain from a controller de-listing under Article 12, such right not being absolute but capable of being granted “*as appropriate*”.
29. Expressly, the Directive carefully circumscribes the territorial scope and application of national law transposing the Directive in Article 4.
30. By contrast, it is notable that there is no legislative provision in the Directive, and no other legislative provision or constitutional rule of Union law, giving the Directive extra-territorial effect as regards any rights or obligations, and, particularly, as regards the right to de-listing and attendant obligations on controllers to de-list, beyond taking steps within the territory where they are established (or a territory where a Member State’s national law applies by virtue of public international law) and, where necessary, other Member States.
31. Ireland submits that, by application of the well-established Union law principle of proportionality, a controller cannot be required to take steps under Article 12 of the Directive that are not directly aimed at meeting the necessary objective of de-listing and which go beyond what is strictly necessary to provide “appropriate” de-listing for a data-subject whose rights have been infringed. In Ireland’s view, it



would be disproportionate and unduly burdensome for operators to be required to ensure global de-listing of a data-subject's data.

32. Further, Ireland submits that, as a matter of general principle, Union law cannot be applied in such a manner as to override data protection law and practice of third countries. The right to be forgotten can only apply within the territorial scope of the Union and there can be no right or expectation on the part of a data subject to have a rule of Union law applied and enforced in third countries. Ireland submits that, to hold otherwise would be contrary to primary and elementary rules of public international law and comity of nations. From the express reference in Article 4(1)(b) of the Directive, evidently it plainly contemplates the taking account and giving effect of conventionally accepted principles of public international law; Ireland submits that this, necessarily, extends to the application of well-recognised rules regarding jurisdiction, territoriality and comity, when applied between Member States, including when acting as the Union, and any third countries.
33. Moreover, where Union law or obligations are properly intended to take effect outside of the Union, this would be expressly provided for by making it clear from the face of legislation that it has an extra-territorial effect or through third-country agreements with the Union.
34. This would prove particularly difficult to impose in circumstances where controllers are themselves required, in the Union, to carry out balancing exercises weighing up whether and how much protection ought to be afforded to a data-subject's rights, and whether it is appropriate to rectify any misuse by the controller. Essentially, this is a delicate balance of privacy of data subjects against freedom of expression and information rights. It is not at all clear how that balance is carried out in third countries and not appropriate or justified to seek to impose standards applied in one or some EU Member States on controllers whose data processing is established or has sufficient effects in third countries. Indeed, it is not clear which third countries do even recognise the existence of a right to be forgotten, or seek to protect it in the same manner as the Directive does.
35. It is a point of some distinction, as a matter of fact, that, in *Google Spain* the CJEU confirmed that the Directive was triggered where search results were

available within a Member State accompanied by advertising directed to consumers in that Member State. Whereas the need to avoid circumvention of the Directive may warrant the application of geo-blocking of searches carried out within the Member State on all domains including .com, Union law cannot be interpreted as requiring the blocking of searches carried out in the territory of a third country.

36. As to the scope of a de-listing decision within the Union itself, Article 4(1)(a) of the Directive confirms that a Member State's law is engaged where processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State. However, a search engine is likely to have establishments in several Member States, in which case the controller is required to take the necessary measures to ensure that each establishment complies with the obligations laid down by the national law applicable.
37. A decision of the supervisory authority of one Member State cannot, however, usurp the jurisdiction of the supervisory authorities of other Member States in which the controller has an establishment. The starting position ought to be that the decision of one supervisory authority ought not to bind the hand of the supervisory authorities of other Member States concerned.

#### **ANSWERS TO QUESTIONS POSED BY THE REFERRING COURT**

38. For the reasons set out above, Ireland submits that the Referring Court ought to answer the questions as follows:

*“1. The scope of the ‘right to de-referencing’, as established by the Court of Justice of the European Union in its judgment in Google Spain of 13 May 2014 on the basis of the provisions of Articles 12(b) and 14(a) of Directive 95/46/EC of 24 October 1995, does not require a search engine, when granting a request for de-referencing, to deploy the de-referencing to all of the domain names used by its search engine so that the links at issue no longer appear, irrespective of the place from where the search initiated; rather, the requirement applies only to searches initiated from within the Union.*”

2. *The 'right to de-referencing' must be interpreted as meaning that a search engine is required, when granting a request for de-referencing to remove, at a minimum, the links at issue from the results displayed following a search conducted on the basis of the requester's name on the domain name corresponding to the State in which the request is deemed to have been made.*
  
3. *In addition to the obligation arising under paragraph 2 above, the 'right to de-referencing' must be interpreted as meaning that a search engine is required, when granting a request for de-referencing, to remove the results at issue, by using the 'geo-blocking' technique, at a minimum, for all searches that are accessible from within the Member State in which the request is deemed to have been made.*

Dated this 7<sup>th</sup> day of December 2017

**Signed: Gemma Hodge**  
**Agent for Ireland**  
**on behalf of Maria Browne, Chief State Solicitor**

**Signed: Tony Joyce**  
**Agent for Ireland**  
**on behalf of Maria Browne, Chief State Solicitor**