INSIGHT

Google v. CNIL: The Territorial Scope of the Right to Be Forgotten Under EU Law

Mary Samonte*

Abstract: This *Insight* provides a critical analysis of the judgment of 24 September 2019, *Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*, case C-507/17, which clarified the territorial scope of the right to be forgotten under current EU law by holding that it only applies within EU borders. Although the Court ruled against an extraterritorial application of the right, the judgment also provides a more nuanced approach in affording legitimacy to a global application of the right. This *Insight* reviews the Court's reasoning and reflects upon the struggles it faced as it decided to set a geographical boundary on a right inextricably linked to the borderless internet. It also discusses the direct impact of the ruling on EU residents seeking to enforce the right and highlights some of its main shortcomings. Lastly, it seeks to assess the judgment's implications toward the status of harmonisation of data protection in the Union.

Keywords: right to be forgotten – data protection and privacy – freedom of expression – territorial scope – internet – State sovereignty.

I. Introduction

In its landmark ruling in case C-507/17, *Google v. Commission nationale de l'informatique et des libertés (CNIL)*,[1] the Court of Justice held that there is no obligation under EU law for Google, and other search engine operators, to apply the European right to be forgotten globally.[2] The decision clarifies that, while EU residents have the legal right to be forgotten, the right only applies within the borders of the bloc's 28 Member States.

* Juris Doctor, Fordham University School of Law; Master of Laws, Université Paris II Panthéon-Assas, msamonte@law.fordham.edu. This *Insight* is based on a blog post in the *European Law Blog* on October 29, 2019.

[1] Court of Justice, judgment of 24 September 2019, case C-507/17, *Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL)*.

[2] *Ibid.*, para. 64.

ISSN 2499-8249
doi: 10.15166/2499-8249/332

In its analysis, the Court considered both the 1995 Data Protection Directive[3] (Directive) and the General Data Protection Regulation[4] (GDPR) which entered into force on 25 May 2018 repealing the Directive.[5] The decision is critical because, at first glance, it appears to have closed the door for EU residents to demand a worldwide removal of their information, under certain circumstances, from search engine results under the GDPR regime. The Court, in this case, decided to set limits on the territorial scope of an individual's right to de-reference. In simple terms, this means that Google is only required to remove links to an individual's personal data from internet searches conducted within the Union.

However, while Google and proponents of the freedom of expression and access to information have claimed this case as an ostensible win, a closer analysis of the Court's decision shows a more nuanced approach which leads to a different conclusion. Although the Court conceded the limitations of current EU law in requiring global de-listing, it also asserted salient points which open the possibility for national courts and data protection authorities (DPAs) in the Union to require search engine operators to de-list globally by recognising their competence to order, where appropriate, the carrying out of a de-referencing on all versions of the search engine. Here, the Court held that Member States and DPAs are competent to balance the right to privacy and protection of personal data against the right to freedom of information in light of national standards of protection of fundamental rights. In this sense, CNIL and other EU national DPAs could, arguably, lay claim to a more substantial victory under this ruling.

I.1. The right to be forgotten

In 2014, the Court of Justice, in *Google Spain*, developed the jurisprudence establishing the European Union law's right to be forgotten,[6] also referred to as the right to de-reference or de-list.[7] It allows individuals in the EU to request search engines to remove links containing personal information from web results appearing under searches for their names.[8] In that judgment, the Court also recognised the need for a balancing test which employs the principle of proportionality to choose between the right to de-list

[3] 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.

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[5] Although the Data Protection Directive was applicable on the date the request for a preliminary ruling was made, it was repealed with effect from 25 May 2018, from which date the GDPR is applicable. Hence, the Court examined the questions in light of both the Directive and the GDPR to ensure that the decision will be of use to the referring court.

[6] Codified at Art. 17 of Regulation (EU) 2016/679.

[7] Court of Justice, judgment of 13 May 2014, case C-131/12, *Google Spain and Google*.

[8] *Ibid.*, para. 93.

and other conflicting rights and interests. It held that the right to be forgotten is not absolute and is granted only when one's personal data protection rights outweigh the public's interest in continued access to the information.[9]

Five years after the development of this legal framework, the territorial scope of this right, *inter alia*, continues to confuse the individuals seeking to enforce it and controllers of processed data receiving requests to de-reference. It is this uncertainty of its territorial scope which prompted France's *Conseil d'État* to seek clarifications from the Court of Justice in case C-507/17.

I.2. Factual and legal background

The case concerned a dispute between Google Inc. and CNIL, the French DPA, with regards to the scale on which de-referencing is to be given effect.

In 2015, CNIL notified Google that it must apply the removal of links from all versions of its search engine worldwide. Google refused to comply and continued to limit its de-referencing of links only on search results conducted in the versions of its search engines with domain extensions within the EU and EFTA[10] and it also added the use of *geo-blocking,* a measure which prevents the links from showing in searches made in France regardless of the version used. CNIL imposed a EUR 100,000 fine on Google for noncompliance. Google then appealed to the *Conseil d'État* seeking to annul the fine. The *Conseil d'État*, noting "several serious difficulties regarding the interpretation of the directive",[11] subsequently referred questions to the Court of Justice for a preliminary ruling concerning the scope of application of Arts 12(b) and 14(a) of the Directive.

The legal framework applicable to privacy and the protection of personal data in the EU at the time of dispute between Google and CNIL was governed by the Directive. The right to be forgotten, in particular, stems from Art. 12(b) which guaranteed every data subject the right to obtain from the controller the rectification, erasure or blocking of processed data which does not comply with the Directive, in particular due to the data being incomplete or inaccurate.[12] The right also developed from Art. 14(a) which granted data subjects the right to object to the processing of data relating to him or her, based on compelling legitimate grounds, except where otherwise provided by national

[9] *Ibid.*, para. 81.

[10] See, *ibid.*, para. 36. The Court notes that the search engine operated by Google is broken down into different domain names by geographical extensions (.fr, .de, .com, etc.). Where the search is conducted from "google.com", Google automatically redirects that search to the domain name corresponding to the State where the search is made. In addition, Google utilises different factors such as the IP address to determine the location of a user performing a search on Google. The search engine will yield different results depending on the domain name extension and location (e.g. through IP address) of the user.

[11] *Google Inc. v. Commission nationale de l'informatique et des libertés*, cit., para. 39.

[12] Art. 12, let. b), of Directive 95/46/EC.

legislation.[13] Under the new EU data protection regime, the right to be forgotten is codified at Art. 17 of the GDPR which gives an individual the right to obtain the erasure of personal data concerning him or her and obliges data controllers to erase said data if it fulfils certain conditions.[14] With the GDPR repealing the Directive on 25 May 2018, the Court analysed the case in light of both the Directive and the GDPR to ensure that the decision will be of use to the referring court.

CNIL contended that for the right to be effective, Google must de-list links universally. It held insufficient both measures implemented by Google to comply with the Directive: *1*) de-listing links from all EU and EFTA extensions, and *2*) de-listing links from all searches conducted in the French territory. CNIL argued that internet users located in France are still able to access the other versions outside the EU (e.g. Google.com). Therefore, removing links about an individual residing in France only from the French version (google.fr) or even from all versions in other EU member states is not enough to protect the individual's right, thereby violating the Directive.

Google argued that CNIL misinterpreted the provisions of the law recognising the right to de-reference by explaining that the right "does not necessarily require that the links at issue are to be removed, without geographical limitation, from all its search engine's domain names".[15] Google contended that CNIL's misinterpretation amounted to a disregard of public international law's principles of "courtesy and non-interference", and the disproportionate infringement of the freedoms of expression, information, communication and the press.

II. The decision of the Court

The Court addressed the question of whether the EU data protection law on de-referencing should be interpreted to mean that a search engine operator is required to remove links either worldwide, or within the EU, or only at the national level. A worldwide de-referencing requires removing links on all versions of its search engine. An EU-wide approach requires the removal of links on versions corresponding to all Member States. A de-referencing at the national level refers to the removal of links only on the version corresponding to the Member State of residence of the person requesting it.[16] The Court also addressed the question of using *geo-blocking* to ensure that an internet user cannot, regardless of the national version of the search engine used, gain access to the links concerned.[17]

[13] Art. 14, let. a), of Directive 95/46/EC.
[14] Art. 17 of Regulation (EU) 2016/679.
[15] *Google Inc. v. Commission nationale de l'informatique et des libertés*, cit., para. 38.
[16] *Ibid.*, para. 43.
[17] *Ibid.*

Taking the side of Google, the Court held that search engine operators are not required under EU law to remove links on all the version of its search engine worldwide.[18] To support its assertion, the Court explained that the texts of the Directive and the GDPR do not indicate that the EU legislature had chosen to confer a territorial scope of the right to be forgotten beyond Member States nor did they intend to impose on search engine operators a de-referencing obligation to include non-EU national versions of their search engines.[19]

Notwithstanding this ruling against an extraterritorial reach of the right to be forgotten, the Court emphasised the EU's goal of providing a high level of protection of personal data throughout the Union as it affirmed an EU-wide application of the right.[20] Accordingly, it held that search engine operators are required to remove all the links on all the versions in the EU regardless of where the request to de-reference originates in the EU.[21]

In addition, the Court held, without specifically mentioning the *geo-blocking* technique used by Google in this case, that search engine operators are required to supplement the de-referencing through measures that would prevent or seriously discourage an internet user located in the EU to gain access to de-listed links when using a search engine version outside the EU.[22]

Notably, even though the Court ruled that EU law did not require search engine operators to automatically de-list links globally, the judgement explicitly permits national courts and DPAs to order, when appropriate, a de-referencing at a global level. In deference to national authorities and DPAs, the Court acknowledged their competence to balance the rights to privacy and data protection against the freedom of information in

[18] *See*, *ibid.*, para. 65. Having regard to all of the foregoing, a search engine operator cannot be required, under Art. 12, let. b), and subparagraph (a) of the first para. of Art. 14, of Directive 95/46 and Art. 17(1) of Regulation 2016/679, to carry out a de-referencing on all the versions of its search engine.

[19] *See*, *ibid.*, para. 62. In particular, it is in no way apparent from the wording of Art. 12(b) and subparagraph (a) of the first para. of Art. 14 of Directive 95/46 or Art. 17 of Regulation 2016/679 that the EU legislature would, for the purposes of ensuring that the objective referred to in para. 54 above is met, have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States and that it would have intended to impose on an operator which, like Google, falls within the scope of that directive or that regulation a de-referencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States.

[20] *Ibid.*, para. 66.

[21] *See*, *ibid.*, para. 73. In the light of all of the foregoing, the answer to the questions referred is that, on a proper construction of Art. 12, let. b), and Art. 14, let. a), of Directive 95/46 and Art. 17, para. 1, of Regulation 2016/679, where a search engine operator grants a request for de-referencing pursuant to those provisions, that operator is not required to carry out that de-referencing on all versions of its search engine, but on the versions of that search engine corresponding to all the Member States, using, where necessary, measures which, while meeting the legal requirements, effectively prevent or, at the very least, seriously discourage an internet user conducting a search from one of the Member States on the basis of a data subject's name from gaining access, via the list of results displayed following that search, to the links which are the subject of that request.

[22] *Ibid.*

the light of national standards of protection of fundamental rights, citing its *Fransson* and *Meloni* jurisprudence.[23]

Finally, as the Court upheld an EU-wide application of the right to be forgotten, it also recognised that even at the EU level the result of balancing the conflicting rights will not necessarily be the same among the Member States.[24] Moreover, it held that the GDPR permits necessary exemptions and derogations at the Member State level with regards to processing for journalistic purposes and artistic or literary expression.[25] Interestingly, the Court also provided Member States a derogation from the required coordination mechanism when de-referencing at the EU level. Under this urgency procedure, a Member State is permitted to unilaterally adopt immediate legal measures on its own territory in order to protect the rights and freedoms of data subjects in exceptional circumstances if done within a specific time frame which will not go beyond three months.[26]

III. Analysis

Google v. CNIL is a long-awaited clarification of, at the very least, the geographical boundaries of the right to be forgotten. As the Court held, there is little room for interpretation under the legal framework of both the Directive and the GDPR to establish a global application of such a right. The judgement was deferential to the legal systems of non-EU nations. It made a point to highlight the difficulties inherent with global de-referencing noting that public interest in access to information substantially vary among third States, therefore, the balancing of fundamental rights would have different results.

The court seemingly faced a difficult choice: either to uphold a global application ensuring full protection under the right, at the risk of jeopardising its legitimacy by encroaching on the sovereignty of third States in balancing fundamental rights, or to rule against an extraterritorial application avoiding a potential overreach, and instead uphold a regional approach to guarantee EU residents the protection of their personal data, albeit limited, within the Union.

Ultimately, the Court went on to say that the EU legal framework on data protection does not provide for cooperation instruments and measures outside its territory[27] and

[23] *Ibid.*, para. 72.

[24] *Ibid.*, para. 67.

[25] *Ibid.*

[26] *Ibid.*, para. 68.

[27] *See, ibid.*, para. 63: "Moreover, although Regulation 2016/679 provides the supervisory authorities of the Member States, in Arts 56 and 60 to 66 thereof, with the instruments and mechanisms enabling them, where appropriate, to cooperate in order to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data concerning him or her against the interest of the public in various Member States in having access to information, *it must be found that EU law does not currently provide for such cooperation instruments and mechanisms as regards the scope of a de-referencing outside the Union"* (emphasis added).

chose the EU-wide approach.[28] Here, the Court made it very clear that it will only impose this particular right within its borders. Nevertheless, in an apparent attempt to mitigate the consequences of a non-universal application, the Court indicated it was not ruling out the possibility that certain cases may justify a global de-referencing.

A key part of the judgment appears to neutralise Google's purported victory in this case. Para. 72 of the judgment reveals the Court's effort to establish the lawfulness of global de-referencing. By finding that EU law does not prohibit worldwide de-listing and that Member States remain competent to order search engine operators to de-reference globally in certain circumstances,[29] the Court leaves open the possibility for France's CNIL and other national DPAs to require global de-referencing in cases where they deem it necessary.

III.1. Implications for EU residents: level of protection

Just because the law stands as it currently does, it does not mean that it is adequate. It can be argued that by explicitly limiting the territorial scope of the right to be forgotten, the Court may have inadvertently limited the impact and full protective effect of this right.

A limit in territorial scope simply means that when an individual residing in the EU requests to have his or her personal information removed from the internet, the links to that exact information will still be accessible to anyone outside the EU and anyone in the EU using a non-EU search engine domain absent effective measures, such as *geo-blocking,* to prevent it. For example, imagine an individual in France requesting Google to de-reference his private information. Under this ruling, Google need only de-reference the relevant links on its EU domains such as google.fr, google.de (.nl, .es, etc.). It does not have to remove the links on non-EU domains such as google.com (.ca, .au, etc.).

In theory, an internet user in France, Germany, the Netherlands and any other Member State would not be able to access the links to web pages containing personal data concerning the French individual who requested the de-referencing. In practice, however, it is highly conceivable that anyone in the EU could still access the de-referenced information through different methods. The easiest of which, given the

[28] *Ibid.*, para. 73.

[29] See, *ibid.*, para. 72: "*Lastly, it should be emphasised that, while, as noted in para. 64 above, EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice*. Accordingly, a supervisory or judicial authority of a Member State remains competent to weigh up, in the light of national standards of protection of fundamental rights (see, to that effect, Court of Justice: judgment of 26 February 2013, case C-617/10, *Åkerberg Fransson*, para. 29; judgment of 26 February 2013, case C-399/11, *Melloni*, para. 60), a data subject's right to privacy and the protection of personal data concerning him or her, on the one hand, and the right to freedom of information, on the other, and, after weighing those rights against each other, to order, where appropriate, the operator of that search engine to carry out a de-referencing concerning all versions of that search engine" (emphasis added).

global reach of the internet, is to have a non-EU internet user perform the search. Another method to access the de-referenced information in the EU is the use of virtual private networks that bypass measures such as *geo-blocking* which prevent internet users in the EU to access the de-referenced links, regardless of which version of the search engine they use.

Furthermore, even if search engine operators are successful in implementing measures that will completely block internet users in the EU from accessing the de-referenced links, the Court had conceded that access, even by non-EU internet users, "to the referencing of a link referring to information regarding a person in the EU is likely to have *immediate and substantial effects* on the person".[30] It markedly declared that due to such substantial effects, the EU legislature has the competence to oblige operators to de-reference links on all versions of its search engines.[31] Arguably, these statements imply that the Court acknowledges that this right can only truly be protected through a universal application owing to the internet's borderless nature.

Therefore, allowing internet users who conduct searches outside the EU to still be able to access the links de-referenced in the EU would potentially undermine the right to be forgotten and weaken the protection sought to be achieved by this right. At a minimum, the Court's ruling implies that the Union's objective of guaranteeing a high level of protection of personal data cannot be fully met under the current law.

III.2. Significance: more than just setting a territorial limit

The importance of this decision also lies in the fact that it has been viewed as a test of whether the EU can extend its data protection and privacy standards beyond its territory.[32] The decision is expected to have broad implications in the regulation of the internet. As companies which process personal data continue to expand their reach on a global scale, the tension between national regulators and these companies is expected to rise.

Without current international standards governing the processing of private information, national jurisdictions are anticipated to try to implement regulations with a global impact and extend their own privacy standards universally to ensure the full protection of their citizens' rights with regards to the processing of personal data.[33] Thus, a legal significance of the Court's ruling is also found on what it will do to reinforce the GDPR's role in setting a standard for international data protection which has significant implications for companies worldwide.

[30] *Ibid.*, para. 57 (emphasis added).

[31] *Ibid.*, para. 58.

[32] *Reuters*: F. Chee, *You have the right to be forgotten by Google – but only in Europe,* 24 September 2019, www.reuters.com.

[33] A.K. Woods, *Litigating Data Sovereignty*, in *Yale Law Journal*, 2018, p. 328 *et seq.*

Moreover, another significant aspect of the judgement which may have a broader implication on the extraterritorial scope of the GDPR beyond the right to be forgotten is the Court's statement that it was no way apparent that the EU legislature would have chosen to confer a scope on the right under Art. 17 of the GDPR to go beyond the territory of the Member States.[34] Here, the Court highlighted the lack of a specific provision in the current EU law that would allow for the application of the GDPR right to be forgotten beyond the EU. By holding so, it appears the Court did not take into account the EU legislature's intention to confer a general extraterritorial application on the GDPR as evidenced by the territorial scope provision under Art. 3, para. 2, of the GDPR.[35]

III.3. A harmonisation or a fragmentation of EU data protection

Incidentally, although the Court's attempt to establish a consistent regulatory standard through an EU-level application of the right was intended to guarantee a high level of protection throughout the EU, the Court may have unintentionally developed jurisprudence that could undermine the EU's goal of harmonising personal data protection across the Union. Allowing national regulators to perform their own balancing test using national standards of fundamental rights to determine a global application will likely create divergent applications among Member States.[36] The lack of an established method to strike the balance between the right to data protection and the right to freedom of information could potentially result in the fragmentation of the level of protection under the GDPR, contrary to its purpose.

Based on the experience with the Directive on data protection, EU legislators concede that the existence of differences in the implementation and application of data protection laws is essentially problematic in attaining the aim of harmonising data protection laws within the EU.[37] Moreover, they noted that these differences create an obstacle in the free flow of personal data throughout the Union affecting the single market. Thus, in response to these issues, the EU adopted the GDPR, a regulation which it deems necessary to provide legal certainty and transparency for economic operators, and to provide all EU residents with the same level of legally enforceable rights.[38] The

[34] *Google Inc. v. Commission nationale de l'informatique et des libertés*, cit., para. 62. In particular, it is in no way apparent from the wording of Art. 12, let. b), and Art. 14, let. a), of Directive 95/46 or Art. 17 of Regulation 2016/679 that the EU legislature would, for the purposes of ensuring that the objective referred to in para. 54 above is met, have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States and that it would have intended to impose on an operator which, like Google, falls within the scope of that directive or that regulation a dereferencing obligation which also concerns the national versions of its search engine that do not correspond to the Member States.

[35] Art. 3, para. 2, of Regulation (EU) 2016/679.

[36] *Google Inc. v. Commission nationale de l'informatique et des libertés*, cit., para. 67.

[37] Regulation (EU) 2016/679, cit., recital 9.

[38] *Ibid.*, recital 13.

GDPR requires that the protection of rights and freedoms of individuals with regards to data processing should be equivalent in all Member States in order to attain a high level of protection. Further, it states that the consistent and homogenous application of the rules for the protection of theses fundamental rights and freedoms should be ensured throughout the Union.[39] The GDPR, by virtue of its nature as a regulation, is directly applicable across the EU. Theoretically, the failure of harmonising data protection laws under the Directive should have been addressed by the GDPR.

However, even though the Court held in this case that, in principle, de-referencing should be carried out in respect to all Member States,[40] the goal of harmonisation does not seem to be met automatically under the GDPR. The potential for fragmentation in the level of protection particularly under the right to be forgotten was recognised by the Court when it held that even at Union level, the weighing up of personal data protection and the public's interest in access to information will vary among Member States.[41] In addition, the Court affirmed that it is for Member States to provide for necessary exemptions and derogations with regards to processing for journalistic purposes and artistic or literary expression.[42] As a consequence, Member States may adopt a different approach under these derogations which could negatively impact the harmonisation of EU data protection law.

On the other hand, in an apparent effort to achieve coherence, the Court did note that the GDPR provides national DPAs with the instruments and mechanisms which enable them to reach a common approach.[43] For cross-border processing, the Court obliged the national authorities concerned to cooperate and reach a single decision binding all DPAs and to provide clear guidelines for search engine operators to follow.[44] Therefore, a divergence in the approach to de-referencing at the Union level obliges Member States to cooperate and reach a binding approach to provide certainty. The effectivity of such cooperation mechanisms among Member States shall be crucial in addressing fragmentation issues that could potentially be caused by deferring to national authorities and DPAs to use national standards to balance rights and permitting derogations from the regulation. Until this happens, search engine operators and data subjects continue to face legal uncertainty and unpredictability.

Further adding to the legal uncertainty is the Court's statement that EU law does not provide for cooperation instruments and mechanisms as regards the scope of a de-referencing outside the Union.[45] This judgement could arguably be interpreted to mean

[39] *Ibid.*, recital 10.

[40] *Google Inc. v. Commission nationale de l'informatique et des libertés*, cit., para. 66.

[41] *Ibid.*, para. 67.

[42] *Ibid.*

[43] *Ibid.*, para. 63.

[44] *Ibid.*, para. 68.

[45] *See*, *ibid.*, para. 63. Moreover, although Regulation 2016/679 provides the supervisory authorities of the Member States, in Arts 56 and 60 to 66 thereof, with the instruments and mechanisms enabling

that a DPA which grants a global de-referencing request does not have to coordinate with other DPAs since a global reach falls outside the Union level and is, therefore, not governed by the obligation to cooperate at the Union level provided under para. 68.

That said, replacing the Data Protection Directive with the GDPR is still poised to further the goal of legislative harmonisation of data protection in the EU. The nature of a regulation, which is binding in its entirety and directly applicable in all Member States,[46] provides an enhanced approach in achieving the desired goal of harmonising laws within the EU. Eliminating the need to transpose a directive into national law decreases the chances of Member States to incorporate the directive differently.

Nonetheless, regulations sometimes give some latitude to Member States and permit them to diverge from the legal standard in certain circumstances. This is a practice which tends to create dissonance instead of harmony. Thus, it is not unexpected to see a regulation not achieve its full scale goal of harmonisation as in this case. Here, the Court found it necessary to provide Member States the flexibility to conduct its own interest and rights balancing test using its own national standards. The degree of diversity this latitude will introduce is yet to be known but the potential for dissonance is significant.

Thus, while the GDPR is a regulation by name and warrants direct applicability, in substance, it is apparent that a significant number of areas in EU data protection law are still left under the discretion of Member States. In fact, the GDPR provides Member States the option to incorporate elements of the Regulation into their national laws.[47] It appears that the potential for divergence in data protection law within the EU is substantial. This case is one such example where a fragmentation of the level of protection is likely to occur under the GDPR as the balancing of rights is left to Member States. Beyond this case, another potential area for fragmentation under the GDPR is the provision giving Member States the discretion to provide, under national law, a different age of consent for a child using online services.[48] Consequently, while the GDPR provides a more harmonised data protection standard compared to the Directive it repealed, it does not seem that it will likely reach its intended purpose of providing complete harmonisation. The practical reality is that data protection laws in Member States is fragmented and it has the potential to continue to diverge even under the GDPR regime. It

them, where appropriate, to cooperate in order to come to a joint decision based on weighing a data subject's right to privacy and the protection of personal data concerning him or her against the interest of the public in various Member States in having access to information, it must be found that EU law does not currently provide for such cooperation instruments and mechanisms as regards the scope of a de-referencing outside the Union.

[46] Art. 288 TFEU.

[47] Recital 8 of the GDPR provides "Where this Regulation provides for specifications or restrictions of its rules by Member State law, Member States may, as far as necessary for coherence and for making the national provisions comprehensible to the persons to whom they apply, incorporate elements of this Regulation into their national law".

[48] Art. 8 of Regulation (EU) 2016/679.

is, therefore, in these areas of divergence, where the role of national law in harmonising data protection in the EU may prove to be more crucial than the GDPR.

Undoubtedly, the GDPR is a significant step towards the right direction in ensuring the consistency and high level of personal data protection appropriate for the digital age. However, this ruling highlights major features inherent in data protection laws which make it difficult to extend their application beyond the jurisdiction of a nation or a region. These features generally involve differences in how third States approach the balancing of fundamental rights of privacy, freedom of expression, access to information, data protection, and more specific to this case, the fact that some third States do not recognise the right to be forgotten. Even within Member States, the Court admits that the results of weighing up the competing rights will not necessarily be the same, posing a challenge to harmonisation if cooperation mechanisms among Member States is not properly implemented.

IV. Conclusion

To conclude, this ruling is noticeably far from the highly publicised victory claimed by Google in the media. Notwithstanding the territorial limits applied in this particular case, it is obvious that the Court's judgment upholds the lawfulness of a global application of the right to be forgotten.

This decision has attracted international interest as it comes at a critical time when the EU's new legal framework in data privacy and protection had just taken effect. Since coming into force, the GDPR has been regarded as having the potential to set the global standard for data protection.[49] It is inspiring third States and data protection authorities around the world to strengthen their own data protection regulations.[50] Certainly, it has placed the rest of the world on notice and global tech companies are keen to identify how its interpretation and enforcement could affect their operations.[51]

This case adds to the legal certainty in relation to the territorial scope of the right to be forgotten but it is just a start in the development of data protection jurisprudence under the GDPR. And while the Court's decision provided clarity on the scope, the absence of clear guidance on how the balancing test among conflicting rights should be assessed will continue to leave areas of uncertainty. It is, therefore, expected that the Court will continue to see more questions about the global reach of the EU's data protection laws.

[49] H. Li, L. Yu, W. He, *The Impact of GDPR on Global Technology Development* in *Journal of Global Information Technology Management*, 2019, p. 1 *et seq.*

[50] T. Ehret, *Data Privacy and GDPR at One Year, A U.S. perspective. Part Two - U.S. Challenges Ahead,* in *Reuters*. 29 May 2019, www.reuters.com.

[51] A. Schildhaus, *EU's General Data Protection Regulation (GDPR): Key Provisions and Best Practices,* in *American Bar Association*, 5 June 2018, www.americanbar.org.

Although this case narrowly focuses on the right to be forgotten, its ruling could have a broader implication on the GDPR's general territorial scope. Beyond search engines, any company which the EU or national regulators regards as providing services that carry out a single act of personal data processing could have all versions of its operations be subject to GDPR's jurisdiction.[52] Indeed, the ruling may have limited the territorial scope of the right to be forgotten but it definitely did not limit that of the GDPR.

The GDPR is significantly changing the landscape of data protection laws around the globe. But the difficulties the Court faced when considering an extraterritorial reach make it clear that the key to implementing a worldwide application of the right to be forgotten is in the development of an international data protection regime which the EU is poised to lead.

It remains to be seen what this decision will do to the development of such a harmonised international data protection regime. What is clear, however, is that the impact of the decision will likely be as important and influential, if not more so, than the decision itself.

[52] The potential application of this reasoning to non-search engine companies in future cases is evidenced by the Court's finding that the GDPR applied to all Google versions, not just Google France. The Court reasoned that because Google's search engine domain names can all be accessed from French territory and, because of the existence of gateways between Google's various national versions, it "must be regarded as carrying out a single act of personal data processing for the purposes applying the Law of 6 January 1978". *See Google Inc. v. Commission nationale de l'informatique et des libertés,* cit., para. 37.