



ELSEVIER

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

**Computer Law
&
Security Review**

Comment

One law to rule them all? The reach of EU data protection law after the *Google v CNIL* case



Emmanouil Bougiakiotis

LL.B (Democritus University of Thrace), MJur, Oxon

ARTICLE INFO

Keywords:

Data protection
Extraterritoriality
International law
Google
Data imperialism
Charter of fundamental rights

ABSTRACT

Google v CNIL is, arguably, one of the landmark cases of EU data protection law and it has been an important development regarding its territorial reach. The judgment's findings in this regard have been controversial and have led to much discussion about their legitimacy and potential repercussions. This paper examines two aspects of this case. First, it considers the holdings of this judgment regarding the global application of EU law in relation to international law and sovereignty. This article argues that though EU decision-makers might have a degree of 'data imperialism' in their thinking, this judgment is not at odds with neither international law nor sovereignty. Second, the paper examines the methodology of the Court and the role it accorded to the Charter of Fundamental Rights of the EU— an aspect that many commentators overlook. In this regard, I argue that the Court's methodology was problematic and that it failed to duly consider the role of the Charter, thus fragmenting EU law.

© 2021 Emmanouil Bougiakiotis. Published by Elsevier Ltd. All rights reserved.

1. Introduction

On May 21, 2015, the President of the French data protection authority, called CNIL, served formal notice to Google, requesting it remove accepted de-referencing requests from the search results of all its domains around the world— effectively a request for global takedowns.¹ This development came as the culmination of a debate that arose in the aftermath of the infamous *Google Spain* case.² In that case, the Court of Justice of the European Union (CJEU) stated that search engines have a duty to remove content, even when the page that is the source

of that content does not— what many have called, erroneously, a right to be forgotten.³ What the Court did not say is to what extent this removal should take place.

There are three main choices available that both the referring court and academics have identified.⁴ The first one is domain based: data controllers can remove the information from specific domains. The second approach is to use geo-filtering techniques, a solution already popular in intellectual property, to identify the location of the user seeking access to informa-

¹ Case C-507/17, *Google LLC v Commission Nationale de l'Informatique et des Libertés (CNIL)* EU:C:2019:772, [2020] 1 CMLR 24, para 30.

² Case C-131/12, *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317 [2014] 3 CMLR 50.

³ *ibid* para 99. See on the use of the term 'right to be forgotten' Orla Lynskey, 'Control over Personal Data in a Digital Age: *Google Spain v AEPD* and *Mario Costeja Gonzalez*' (2015) 78 MLR 522, 528.

⁴ *Google v CNIL* (n 1) para 39; Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and Jurisdiction after *Google Spain*: The Extraterritorial Reach of the "Right to Be Delisted"' (2015) 5 IDPL 105, 111; Emmanouil Bougiakiotis, 'The Enforcement of the *Google Spain* Ruling' (2016) 24 JLLIT 311, 329–30; Andrew Keane Woods, 'Litigating Data Sovereignty' (2018) 128 Yale LJ 328, 374–78.

tion and show the appropriate results.⁵ Both solutions can apply either to the home state of the data subject or across the EU. Lastly, and much to the dismay of Internet companies, a third option is to remove the results from all domains—effectively implementing EU data protection rights globally.⁶ There are also some proposals that involve a mixture of these solutions.⁷

Following *Google Spain*, Google set out to address this issue. It initially removed results from all EU domains.⁸ However, this dissatisfied European regulators, as anyone could easily access the removed information through a non-EU domain. As a result, Google adopted the stronger geo-filtering approach.⁹ Nevertheless, regulators remained unconvinced and the Article 29 Working Party, the collective body of EU data protection authorities, issued guidelines that called for global de-listing.¹⁰

Since data protection governance remains decentralized in Europe, national authorities can adopt their own interpretations of data protection laws within their jurisdictions.¹¹ Hence, CNIL pressured Google to implement global take-downs. Google refused, pointing to its geo-blocking proposal as an effective alternative. Though other regulators accepted this, CNIL insisted and issued a fine of €100,000 against Google.¹² Google then sought to annul this decision before the supreme French administrative court, the Conseil d'Etat.¹³

When the case reached that court, the latter was obliged to use the preliminary reference procedure.¹⁴ The referring court presented the CJEU with the three options mentioned above.¹⁵ It also conveyed Google's objections, which were twofold. First, Google argued that neither Directive 95/46/EC, nor the *Google*

Spain ruling required global removals. In addition, it argued that such an implementation would contradict 'principles of courtesy and non-interference recognized by public international law' and the freedoms of expression, of communication, and of the press.¹⁶

The CJEU's judgment on the preliminary reference request first clarified that, though the case arose under Directive 95/46, it would decide it considering the GDPR as well, to ensure that its answers would be relevant in any case.¹⁷ Of course, one would expect that the question of which law is applicable concerns the interpretation of European law, but the Court did not address it. In any case, having clarified the applicable laws, the Court proceeded by re-affirming its main findings in *Google Spain*.¹⁸ This clearly demonstrates, the strong link between the two cases: *Google v CNIL* essentially continues from where *Google Spain* finished.

After setting the background, the Court identified two main countervailing considerations in its judgment. The first one is the need for the effective protection of personal data,¹⁹ which has, controversially, been accorded great weight in the Court's recent case law.²⁰ The Court noted that access to a data subject's data relating to a person 'whose centre of interests is situated in the Union is [...] likely to have immediate and substantial effects on that person within the Union itself', in line with its past jurisprudence.²¹ It also hastened to add that this interest would justify the imposition of global take-downs by the EU legislature, before even turning to the opposite considerations.²² Reaching such a conclusion in this manner is bizarre, especially since, per the Court itself, data protection is not absolute.²³ It does reflect, however, the Court's strong, pro-privacy approach.

The main opposite interest that the CJEU acknowledged was the difference between the EU and other states on how they strike a balance between freedom of expression and the right to de-referencing.²⁴ Implicitly, the Court seems to acknowledge in this manner the points raised by Google about foreign sovereignty. In this respect, the Court stressed that as data protection is not an absolute right, it is subject to the proportionality principle and that the balance struck between data protection and freedom of expression can vary significantly across the world.²⁵ Practically, these observations are relevant only regarding the Court's balancing. As far as the

⁵ See generally Thomas Schultz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 819–28.

⁶ See, e.g. Peter Fleisher, 'Adapting Our Approach to the European Right to Be Forgotten' (*Google- The Keyword*, 4 March 2016) <<https://blog.google/around-the-globe/google-europe/adapting-our-approach-to-european-right-to-be-forgotten/>> accessed 24 July 2020; Peter Fleisher, 'Three Years of Striking the Right (to Be Forgotten) Balance' (*Google- The Keyword*, 15 May 2017) <<https://blog.google/around-the-globe/google-europe/three-years-right-to-be-forgotten-balance/>> accessed 18 December 2020.

⁷ See, e.g. Bougiakiotis (n 4) 330 arguing for geo-filtering as the default and for balancing to expand or decrease the scope of application, which is similar to the Court's decision.

⁸ Fleisher, 'Adapting Our Approach' (n 6).

⁹ *ibid.*

¹⁰ Article 29 Working Party, 'Guidelines on the implementation of the Court of Justice of the European Union judgment on "Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez" C-131/12', (2014) WP 225 para 20.

¹¹ See generally 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) [2016] OJ L119/1, ch VII (GDPR).

¹² *Google v CNIL* (n 1) para 33.

¹³ *ibid* para 34.

¹⁴ Treaty on the Functioning of the European Union [2012] OJ C326/1, Art 267 (TFEU).

¹⁵ *Google v CNIL* (n 1) para 39.

¹⁶ *ibid* para 38.

¹⁷ *ibid* para 41.

¹⁸ *ibid* paras 44–45.

¹⁹ *ibid* paras 56–57.

²⁰ *Google Spain* (n 2); Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* [2014] ECR I-238; Case C-362/14 *Schrems v Data Protection Commissioner* [2015] ECR I-650. See for criticism against the Court Dawn Carla Nunziato, 'The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten' (2018) 39 U Pa J Int'l L 1011; Stefan Kulk and Frederik Zuiderveen Borgesius, 'Google Spain v. Gonzalez: Did the Court Forget about Freedom of Expression' (2014) 5 Eur J Risk Reg 389; Ignacio Cofone, 'Google v. Spain: A Right to Be Forgotten' (2015) 15 Chi-Kent J Int'l & Comp L 1.

²¹ *Google v CNIL* (n 1) para 57.

²² *ibid* para 58.

²³ *ibid* para 60.

²⁴ *ibid* paras 59–60.

²⁵ *ibid* para 60.

legislature is concerned, the CJEU already indicated that it has the liberty to draw the line wherever it deems fit.

Though the Court had set the ground for balancing these two opposing interests, it suddenly changed its approach, proceeding in a very conservative manner. Although the legislature has struck a balance between data protection and freedom of expression as far as the EU is concerned, the Court said, it has not yet done so regarding the rest of the world.²⁶

It then added that 'it is in no way *apparent from the wording* of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46 or Article 17 of Regulation 2016/679 that the EU legislature would, for the purposes of ensuring that the objective referred to in paragraph 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.'²⁷

It also noticed that while there is a mechanism for the cooperation of data protection authorities in order to impose de-referencing within the Union, this does not seem to be the case for de-referencing beyond it.²⁸

The Court then turned its attention to the question of whether the de-listing should take place in the member state of residence of the data subject or throughout the EU. The CJEU decided that to ensure both a consistent and high level of protection of rights and the free flow of data, de-listing should take place 'in principle' in all member states.²⁹ However, it acknowledged that the balance struck between the right to privacy and access to information might vary from one member state to another, given that they determine freedom of expression derogations.³⁰ Hence, in cross-border cases these differences will be reconciled through the procedure described in Chapter VII of the GDPR.³¹ This Chapter provides for the cooperation of the data protection authorities involved within the framework of the European Data Protection Board (EDPB), their collective body. The Court added that search engines must also take measures to ensure the effective protection of the data subject's rights having 'the effect of preventing or, at the very least, seriously discouraging' unwarranted access to her data.³²

Before concluding, however, the Court added one more basis for global removals, arguing that EU law might not currently require them but it also does not prohibit them. Therefore, national authorities are free to require such action pursuant to national human rights provisions.³³ This last paragraph changes the effect of the entire judgment. Though the

court left the door open for EU law to impose global removals, it recognized no such obligation as things stand, depriving data protection authorities from a basis to enforce such removals. Their only option would be to wait for EU institutions to give them such power through legislation, a time consuming and politically difficult endeavor. However, by allowing them to make such orders based on national human rights provisions, the Court allowed for national authorities to issue takedown orders based on their national law.

This Comment discusses two main issues about this judgment. The first one is outward looking and has to do with concerns about foreign sovereignty and whether this ruling is compatible with international law. The second one has to do with the methodology the Court used in this case and the dangers for potential fragmentation of EU law. Both issues have been grounds for strong criticism against the Court. However, I will argue that, contrary to popular belief, the Court was mostly right on the first issue and mostly wrong on the second. Specifically, I will argue that the claims that this ruling violated the sovereignty of other states are in large part baseless, although the accusation of ideological imperialism stands on more solid ground. In addition, I aim to demonstrate that this judgment was methodologically erroneous and that the Court failed to provide necessary guidance by adopting a very narrow approach that compromised EU fundamental rights. However, I will also argue that the fragmentation of EU law and the problems this judgment might create to its harmonization are largely not the Court's fault.

2. Data imperialism, sovereignty, and international law

2.1. Why the court did not violate sovereignty

When the CJEU announced its judgment on this case, many people perceived it as a win for Google and a brake on the rapid expansion of data protection in the CJEU's case law.³⁴ However, one can read this judgment in another manner.³⁵ The Court may not have allowed EU law-based global de-listing, but it acknowledged two other bases that might be even more effective.

To begin with, as mentioned above, the Court gave almost a *carte blanche* to EU legislators to expand the de-listing pursuant to data protection law as they wish. It is telling that the Court put forward that statement whilst examining the need for effective data protection and before even introducing the

³⁴ See eg Lio Kelion, 'Google Wins Landmark Right to Be Forgotten Case', (BBC News, 24 September 2019) <<https://www.bbc.com/news/technology-49808208>> accessed 28 December 2020; 'Google Wins Privacy Case' (New Law Journal, 25 September 2019) <<https://www.newlawjournal.co.uk/content/google-wins-privacy-case>> accessed 28 December 2020.

³⁵ Hunter Criscione, 'Forgetting the Right to Be Forgotten: The Everlasting Negative Implications of a Right to Be Dereferenced on Global Freedom in the Wake of Google v. CNIL' (2020) 32 Pace Int'l L Rev 315, 333-37; Tu Huynh, 'Google LLC v. Commission Nationale de l'Informatique et Des Libertes (CNIL): Does Everyone Have to Listen to the European Union?' (2020) 28 Tul J Int'l & Comp L 359, 369.

²⁶ *ibid* para 61.

²⁷ *ibid* para 62 (emphasis added).

²⁸ *ibid* para 63.

²⁹ *ibid* para 66.

³⁰ *ibid* para 67.

³¹ *ibid* para 68.

³² *ibid* para 70.

³³ *ibid* para 72.

opposite concerns for foreign sovereignty. In other words, the Court acknowledged this unlimited power of the EU without even purporting to engage in any balancing.

Given this, the objection that the Court did not accord equal weight to sovereignty interests is valid.³⁶ I would go even further—the Court did not actually seem to balance the opposing interests at any stage. It simply mentioned these interests in passing, and it reached its conclusions *before* and *after* setting the stage for a balancing that never came. How then, one might wonder, can I argue that it did not violate sovereignty? To answer this question, one must bear in mind the rules of international law that apply in this case. Those are very difficult to ascertain.

Rules of jurisdiction are notoriously fuzzy in international law. The classical case that every relevant analysis has as a starting point is *Lotus*.³⁷ The traditional perception of that case in public international law is that what the law does not prohibit, it permits. Although there is certainty that direct enforcement of foreign laws in another country's territory is beyond bounds, mainstream international law scholarship considers the exercise of prescriptive jurisdiction, which is subjecting entities or persons of one state to another state's law, as legitimate.³⁸ Paradoxically, however, this reading of the case is the one that the dissenting minority used to rebut it.³⁹ The wording of the majority is notoriously elusive and it is doubtful whether this reading reflects it. Hence, there are also other readings of this judgment, which complicate things.⁴⁰

As if this was not enough, whether this case remains good law is unclear. Some scholars argue that customary international law developments deem *Lotus* no longer valid and that some bona fide connection between the state that exercises jurisdiction and its subject matter is necessary.⁴¹ Under this view, if more states have a connection to a matter, then some sort of balancing ought to take place to identify which state should take precedence.⁴² Though there are some indications, it is far from clear which connection is stronger or what kind of test is suitable to carry out this balancing. What is more, balancing is famously difficult to pin down and highly subjective.⁴³ It really is no wonder that the Court avoided entering this spiral.

However, I am not saying that the Court did not violate foreign sovereignty because it did things right, “right” being here a very ambiguous concept. I am saying that the Court did not do enough in its ruling for it to amount to a violation. Sure,

the Court did not set any substantive limits that derive from sovereignty, neither for EU organs, nor for national ones. However, both of them do not need the Court to reiterate them—this is an obligation that they have regardless.⁴⁴ What is more, the Court did include a relevant passage in its judgment that it can point to if it needs to tighten the rope, despite the fact that it plays no substantial role in it.⁴⁵

When viewed from a broader perspective, the Court's judgment has actually managed, in a way, to strike the right balance. It provided for the broadest possible protection that does not infringe foreign interests as the default, i.e. geo-filtering across all member-states. Some cases will require deviations, either internally, because the value of information is different in some member-states, or externally, because the balance between the interests in protecting personal data trumps foreign interests against a global injunction. Balancing will have to take care of that. The caveat here is that the balancing is left completely to national authorities, which can cause problems— I will return to this point later on.

2.2. The (Lack of a) danger of a regulatory race to the bottom

Another complaint about the CJEU's decision is that by providing for global removal of information the Court allowed other countries, which might have totalitarian regimes, to use this as precedent. Hence, the argument goes, these countries might utilize this as a legal basis to retaliate against Western democracies as well as to impose their illiberal agenda. It is noteworthy that besides academics,⁴⁶ officials,⁴⁷ and tech companies,⁴⁸ the Advocate General himself supported this argument in his Opinion.⁴⁹ If we go down this road, he warned, we will start a regulatory race to the bottom where every state seeks to secure global domination over the Internet by introducing increasingly expansive laws. In arguing so, the Advocate General cited the Opinion of his predecessor in *Google Spain*, where the latter argued that there is an increasing need

⁴⁴ ILC, 'Draft articles on Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10 Art. 4.

⁴⁵ *Google v CNIL* (n 1) paras 59–60.

⁴⁶ Krystyna Kowalik-Bańczyk and Oreste Pollicino, 'Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information' (2016) 17 *German LJ* 315, 336; Daphne Keller, 'Ominous: Canadian Court Orders Google to Remove Search Results Globally' (*Center for Internet and Society- Stanford Law School*, 28 June 2017) <<http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally>> accessed 27 January 2021; Matthew Marinett, 'The Race to the Bottom: Comity and Cooperation in Global Internet Takedown Orders' (2020) 53 *UBCL Rev* 463; Ronald J Krotoszynski Jr, 'Privacy, Remedies and Comity: The Emerging Problem of Global Injunctions and Some Preliminary Thoughts on How Best to Address It' in András Koltay and Paul Wragg (eds), *Comparative Privacy and Defamation* (Edward Elgar Publishing 2020) 310.

⁴⁷ UNHRC, 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' UN Doc A/HRC/38/35 para 18.

⁴⁸ Fleisher, 'Three Years of Striking the Right (to be Forgotten) Balance' (n 6).

⁴⁹ Case C-507/17, *Google LLC v Commission Nationale de l'Informatique et des Libertés (CNIL)* EU:C:2019:772, [2020] 1 *CMLR* 24 Opinion of AG Szpunar, para 61.

³⁶ cf Criscione (n 35) 332.

³⁷ *The Case of the SS Lotus (France v Turkey)* PCIJ Rep Series A No 17.

³⁸ *ibid* at 19; Cedric Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015) 9.

³⁹ *Lotus* (n 37) 60 (Nyholm, J). cf *ibid* at 42 (Weiss, J).

⁴⁰ Frederick Alexander Mann, *The Doctrine of Jurisdiction in International Law* (AW Sijthoff 1964) 35; AV Lowe, 'Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980' (1981) 75 *AJIL* 257, 263; An Hertogen, 'Letting Lotus Bloom' (2015) 26 *EJIL* 901.

⁴¹ Mann (n 40) 35, 46; Ryngaert (n 38) 29, 34–36, 43.

⁴² Ryngaert (n 38) ch 5.

⁴³ Stavros Tsakyrakis, 'Proportionality: An Assault on Human Rights?' (2009) 7 *ICON* 468; Timothy Endicott, 'Proportionality and Incommensurability' in Grant Huscroft and others (eds), *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (CUP 2014).

for the protection of free speech in light of the authoritarian regimes' tendency to limit Internet access and censure its contents, thus indirectly endorsing the fear of retribution from them.⁵⁰

There are three reasons that make this argument unconvincing. First, not only are global injunctions anything but new in general, but such orders, concerning the Internet in particular, have been around for some time.⁵¹ Most of the states that have issued them are not totalitarian outcasts of the international community seeking to usurp Internet domination. They are rather western democracies seeking to protect well-accepted national norms of a commercial or fundamental rights nature, even if their specific manifestation is not universal.⁵² Therefore, those supporting this argument have the onus to demonstrate not only why the dangers they describe concern the Internet exclusively, in the extent that they do not argue against global injunctions in general, but also why this regulatory conflict has not yet taken place although this practice has already materialized in various parts of the world. Unfortunately, there have been no arguments in this regard so far.

Second, when states issue global removal orders, even if they have no geographical limitations, they do take into account foreign interests and comity concerns, although the weight they accord to them varies. Even the *Google v CNIL* judgment, with all its shortcomings, acknowledged such interests and, as I argued above, one should expect that EU member-states will consider them when they seek to apply data protection law overseas.⁵³ It is telling that those concerned about a regulatory race to the bottom and the infringement of foreign sovereignty frame their arguments in *abstracto*, without citing any relevant precedent of such malicious state action.⁵⁴

It does not follow that a sensible decision that adequately, or even inadequately, balances foreign interests will provide a legal basis for other states to impose global injunctions without good reason. Specifically, it is doubtful that such a decision would provide other states with legal grounds for such action as countermeasures, especially if they concern the entirety of the Internet and the state exercising jurisdiction has no links to the subject matter or consideration of foreign interests.⁵⁵ No doubt, there are good reasons to worry about imposing conflicting obligations and, hence, it makes sense to

call for the use of comity and respect for foreign sovereignty in judicial decisions. However, comity by no means entails abstaining from exercising global jurisdiction and it does require that we examine the various interests at stake in *concreto*.⁵⁶

Third, and perhaps most importantly, such means are unlikely to be suited to serve the purposes of taking control over the Internet globally.⁵⁷ The procedures that apply to issuing injunctions and having them recognized abroad are not particularly efficient. Domestic courts will have to issue an injunction and then foreign courts will have to recognize it. This process is quite time consuming and easily evadable by distributing information from other jurisdictions that have not recognized such judgments. Furthermore, courts do not implement judgments that are contrary to the public policy of the recognizing state.⁵⁸ Obviously, they are unlikely to recognize foreign judgments that award global injunctions in order to retaliate or to promote the suppression of information or that interpret rights in a substantively detrimental manner for the rights of the recognizing state's citizens.⁵⁹

Moreover, it is unlikely that such regimes will have the market power to force Internet giants to comply. It is one thing to threaten such companies into submission regarding their operation within a state, eg what China did,⁶⁰ and another to make them act in violation of human rights across the globe.⁶¹ In such a collision scenario, the combined economic and polit-

⁵⁶ Woods (n 4) 390–92.

⁵⁷ Jonathan Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' in Adam Thierer and Clyde Wayne Crews Jr. (eds), *Who Rules the Net?: Internet Governance and Jurisdiction* (Cato Institute 2003) 21.

⁵⁸ See eg Restatement (Third) of the Foreign Relations Law of the United States § 482(2)(d) (Am. Law Inst. 1987); Regulation (EU) 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters [2012] OJ L351/1, Art 45(1)(a); Woods (n 4) 392.

⁵⁹ This depends in part on the horizontality of human rights and on whether internet intermediaries have freedom of expression rights. For instance, some authors in the US argue that US courts could recognize foreign judgments imposing global injunctions because there is no obligation under US law for such companies to provide specific content see Krotoszynski Jr (n 46) 312–13. However, there is already precedent to the contrary see *Yahoo! Inc v La Ligue Contre Le Racisme* (n 51); *Google LLC v Equustek Solutions Inc* WL 5000834 (ND Cal). See also Leslie E Minora, 'US Courts Should Not Let Europe's Right to Be Forgotten Force the World to Forget' (2017) 89 Temp L Rev 609; Woods (n 4) 392. Regarding Europe, the CJEU has acknowledged that the freedom of information is at play, see *Google v CNIL* (n 1) 60. See also *Delfi AS v Estonia* (2016) 62 EHRR 6, para 115 regarding the European Court of Human Rights.

⁶⁰ See eg Jyh-An Lee and others, 'Searching for Internet Freedom in China: A Case Study on Google's China Experience' (2013) 31 Cardozo Arts & Ent LJ 405, 426–28.

⁶¹ Zittrain (n 57) 21. cf Paul M Schwartz, 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (2013) 126 Harvard L Rev 1966, 1985–90 noting the limitations of even the EU 'Brussels effect' to unilaterally determine world standards citing Anu Bradford, 'The Brussels Effect' (2012) 107 Nw UL Rev 1. See also Mercy A Kuo, 'The Brussels Effect and China: Shaping Tech Standards' (*The Diplomat*, 7 January 2020) <<https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/>> accessed 27 January 2021 interviewing Bradford who mentions that China has a more limited regulatory capacity compared to the EU.

⁵⁰ *ibid* at 61 citing Case C–131/12, *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)*, Mario Costeja González, EU:C:2014:317, [2014] 3 CMLR 50 Opinion of AG Jääskinen, para 121.

⁵¹ *Yahoo! Inc v La Ligue Contre Le Racisme* 433 F 3d 1199 (9th Cir 2006); *Google Inc v Equustek Solutions Inc* [2017] SCC 34; *OmniGEN Research v Wang* 2017 WL 5505041, para 279 (Dist Court, D Oregon 2017). See also Woods (n 4) 390 explaining how anti-suit injunctions are also in essence global injunctions.

⁵² *ibid*.

⁵³ *Google v CNIL* (n 1) paras 59–60.

⁵⁴ See n 46–49.

⁵⁵ According to *Case Concerning the Gabcikovo-Nagymaros Project* (Hungary v Slovakia) [1997] ICJ Rep 7, paras 83, 85 a countermeasure must be directed against a state that took an internationally wrongful action and be commensurate to it. If totalitarian states introduce countermeasures that affect third-states or that are more infringing than the injury they suffered, they will be unlawful.

ical influence of Western democracies will prevail. In any case, such regimes seem keener on controlling the flow of data inside their borders than on suppressing access to information abroad.⁶² If anything, they use the abundance of information in Western democracies to create misinformation, as it has recently become clear.⁶³

2.3. Why the court might be guilty of data imperialism

During the first years of the Internet, many people viewed it as a groundbreaking medium that challenged existing societal structures. Its borderless nature, its unprecedented accessibility, and its evasiveness of the enforcement of laws (at least at that time), led to the development of some accounts of it as a new, self-governed or even anarchic online society.⁶⁴ Although many of the predictions of these cyber-prophets did not materialize, the ideal of an Internet with light or no state regulation persists and it has at times played a significant role in how states develop their approaches.⁶⁵ Woods has termed this ideal as cosmopolitan, whilst Zittrain has used the simpler term 'global law'.⁶⁶ Both terms generally stand for the ideal of a universal set of rules, be it binding or not, that release Internet actors from following state rules and ensure that the Internet is free. The crucial question then becomes which rules apply. Absent state regulation, Woods correctly points out, those will be the laws of the state that governs Internet intermediaries, in most cases American, either because they embrace the same values as their home state or because of the government's influence.⁶⁷

By contrast, the opposite approach is the sovereign deference ideal that advocates for the application of local law over different parts of the Internet.⁶⁸ This idea is based on an unexceptionalist perception of the Internet, considering it to be

no different than any other subject matter.⁶⁹ Therefore, according to this argument, regulating the Internet should not differ from any other subject matter where states exercise their authority. Professor Woods has made an additional argument in favor of sovereign deference. Its main premise is that states are going to eventually manage to subdue the Internet to their will, if need be through asserting control over its infrastructure. Hence, deferring to them is preferable since it will allow them to assert their sovereignty through cooperation with their international partners and without them having to resort to more drastic measures, thus preserving a greater degree of freedom.⁷⁰

The EU's views do not align exactly with either of those approaches. Though it certainly is not in favor of allowing the Internet to operate without state regulation, there are important hints that it also does not aim exclusively at retaining control over intraterritorial activities. There seems to be a third trend rising in the EU which seeks the global implementation of European data protection standards. This trend has manifested itself in various forms both in regulatory⁷¹ and judicial⁷² decisions, the case at hand being a prominent example, and in statements by EU officials who seek to establish its law as a model for data protection regulation abroad.⁷³

To be clear, none of the official actions taken by the EU is necessarily at odds with sovereign deference, nor does it mean that the EU is trying to impose its views on the world. As mentioned before, global injunctions do not per se contravene the

⁶² Shannon Tiezzi, 'China's "Sovereign Internet"' (*The Diplomat*, 24 June 2014) <<https://thediplomat.com/2014/06/chinas-sovereign-internet/>> accessed 26 February 2021; Alexandra Ma, 'Russia Officially Introduced a "Sovereign Internet" Law to Let Putin Cut Off the Entire Country from the Rest of the Web' (*Business Insider*, 1 November 2019) <<https://www.businessinsider.com/russia-sovereign-internet-law-cut-web-access-censorship-2019-11>> accessed 26 February 2021.

⁶³ See eg Mark Scott, 'Russia and China Push "Fake News" Aimed at Weakening Europe: Report' (*Politico*, 1 April 2020) <<https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/>> accessed 15 July 2020.

⁶⁴ John Perry Barlow, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <<https://www.eff.org/cyberspace-independence>> accessed 25 February 2021. See also David R Johnson and David Post, 'Law and Borders: The Rise of Law in Cyberspace' (1996) 48 *Stan L Rev* 1367.

⁶⁵ See eg William J Clinton and Albert Gore Jr., 'A Framework for Global Electronic Commerce' (*The White House*, no date) <<https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>> accessed 21 January 2021; United States Department Of State, 'Global Internet Freedom Task Force' (Department Of State, The Office of Electronic Information, Bureau of Public Affairs 2001–09,) <<https://2009.state.gov/g/drl/lbr/c26696.htm>> accessed 21 January 2021.

⁶⁶ Zittrain (n 57) 21; Woods (n 4) 359.

⁶⁷ Woods (n 4) 367.

⁶⁸ *ibid* also uses the term 'sovereign difference'.

⁶⁹ Jack L Goldsmith, 'Against Cyberanarchy' (1998) 65 *U Chi L Rev* 1199; Jack L Goldsmith, 'Against Cyberanarchy' in Adam Thierer and Clyde Wayne Crews Jr (eds), *Who Rules the Net?: Internet Governance and Jurisdiction* (Cato Institute 2003); Alex Kozinski and Josh Goldfoot, 'A Declaration of the Dependence of Cyberspace' (2008–09) 32 *Colum JL & Arts* 365; Andrew Keane Woods, 'Against Data Exceptionalism' (2016) 68 *Stan L Rev* 729.

⁷⁰ Woods (n 4) 371.

⁷¹ See Article 29 Working Party (n 10).

⁷² See n 20.

⁷³ Giovanni Buttarelli, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 *IDPL* 77; Jan Phillip Albrecht, 'How the GDPR Will Change the World' (2016) 2 *EDPL* 287; Adam Satariano, 'G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog', *The New York Times* (24 May 2018) <<https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html>> accessed 8 July 2020 asserting that 'European officials are encouraging copycats by tying data protection to some trade deals and arguing that a unified global approach is the only way to crimp Silicon Valley's power'; Mark Scott and Laurens Cerulus, 'Europe's New Data Protection Rules Export Privacy Standards Worldwide' (*Politico*, 31 January 2018) <<https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>> accessed 21 January 2021 quoting Commissioner Jourová saying '[w]e want to set the global standard'. cf European Commission, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM (2020) 264 final at 3 stating that '[t]he EU's leadership on data protection shows it can act as a global standard-setter for the regulation of the digital economy. . .'. But see Michael L Rustad and Thomas H Koenig, 'Towards a Global Data Privacy Standard' (2019) 71 *Fla L Rev* 365 considering the GDPR as a mixture of EU and US approaches.

sovereignty of other states. The same applies a fortiori to adequacy decisions, which only concern the actions of the EU and its member-states, and to international agreements, for which other states have to provide consent.⁷⁴ Turning to the case at hand, one can argue that the Court was merely asserting the legitimate interest of the Union in the protection of personal data. After all, contrary to the cosmopolitan view, the EU has not publically advocated for the global application of a single set of rules on the Internet.

However, I think that if one reads behind the lines of various statements and combines them together, this intention might be discernible. Some EU officials have pretty much admitted so openly.⁷⁵ Of course, there is no way to know the degree in which the Court shares these aspirations. Nevertheless, there are some strong indications in its ruling that it does. In particular, the fact that its consideration of foreign interests was minimal and that it sought at no point to set some boundaries for the EU legislature or national authorities to pursue this path is telling. This does not mean that the effects of this judgment were imperialist, in the sense that it imposed EU law in general on third states. It did not, at least not directly.⁷⁶ Nor is it certain that without this approach the Court would have reached a different result. Nevertheless, entertaining that idea does not seem unreasonable.

Even if they agree with my analysis, a lot of European data protection experts, might disagree with the data imperialism characterization. It is beyond doubt that the EU has been a pioneer in this field and that, as such, it has had a strong influence on how other states approach data protection.⁷⁷ That is not bad per se. Yet, it seems that sometimes the EU seeks to expand the influence of its rules, be it through unilateral action or by promoting their adoption abroad, not merely to protect its own interests or to share its know-how, but because of an implicit belief in the superiority of its own system. Regardless of the merits of this belief, however, there might be important reasons that justify other states adopting a different approach. To use the Razian terminology, this seems to be a first-order argument that ignores the second-order ones.⁷⁸ In other words, as sound as EU data protection law might be,

and that is an open question, there might be legitimate reasons that do not relate to its merits for not following it.⁷⁹

The EU's pursuit of making its laws the 'gold standard' of data protection regulation may be well-intentioned. However, it can have significant adverse consequences. First, it may not allow third-states to adopt laws that better reflect the particular characteristics of their legal system. It is no doubt true, that EU data protection law is groundbreaking and has, hence, been a source of inspiration for other states. However, in trying to extend its influence beyond that, the EU might be wasting its political capital on a vanity project. Besides the fact that it devotes resources towards a goal that is unlikely to yield fruitful results, this could also have an impact on its future influence. After all, it is no coincidence that the term data imperialism has been increasingly associated with it. This might be a regrettable development as global cooperation on data governance starts to gain pace, in which the EU's contribution can be particularly useful.

3. Methodological errors and the Fragmentation of EU law

3.1. The court's flawed interpretive methodology

The CJEU, following the continental European tradition, has used several methods of interpretation in its case-law throughout the years. Koen Lenaerts, the President of the Court and its Vice-President at the time, along with his legal secretary José Gutiérrez-Fons, wrote an important piece on the interpretative methods that the Court uses.⁸⁰ In their article, they examine various cases of the Court and they identify three main modes of interpretation. The first one is textualist, the second one is contextual, and the third one is teleological. In a typical fashion, the authors acknowledge that the Court must combine all these methods in accordance with the EU's objectives, without any of them being preferable a priori.⁸¹

An exception to this rule is arguably made for the textual approach. As the Court acknowledged in *CILFIT*, if a provision is clear, there is no need to consider anything else than its text.⁸² Of course, when the text contravenes the Union's objectives, judges can move beyond it to reconcile them.⁸³ The second mode of interpretation focuses on context. In this respect, the Court has interpreted the law based on a systematic approach that tries to make sense of the various provisions by examining them in conjunction and interpreting them to

⁷⁴ See Paul M Schwartz, 'Global Data Privacy: The EU Way' (2019) 94 NYUL Rev 771, 804, 807. cf Orla Lynskey, 'Extraterritorial Impact in Data Protection Law through an EU Law Lens' (2020) Brexit Institute Working Paper Series No 8/2020 <<https://papers.ssrn.com/abstract=3674413>> accessed 6 August 2021. But see Scott and Cerulus (n 73); Theodore R Bromund, 'The U.S. Must Draw a Line on the EU's Data-Protection Imperialism' (*The Heritage Foundation*, 9 January 2018) <<https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism>> accessed 29 January 2021; Cara Mannion, 'Data Imperialism: The GDPR's Disastrous Impact on Africa's E-Commerce Markets' (2020) 53 Vand J Transnat'l L 685.

⁷⁵ Buttarelli (n 73); Albrecht (n 73); Scott and Cerulus (n 73).

⁷⁶ See Federico Fabbrini and Edoardo Celeste, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German LJ 55, 64 arguing that the Court's judgement was 'a pragmatic solution, which tries to navigate between the Scylla of data protection imperialism and the Charybdis of digital sovereignty'.

⁷⁷ See eg Schwartz (n 74).

⁷⁸ Joseph Raz, *Practical Reason and Norms* (OUP 1999) s 1.2.

⁷⁹ See Alessandro Mantelero, 'The Future of Data Protection: Gold Standard vs. Global Standard' (2021) 40 CLS Rev 105500 forthcoming arguing that the strong influence of the EU might deter some countries from adopting it in contrast to other regional instruments.

⁸⁰ Koen Lenaerts and José A Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Colum J Eur L 3.

⁸¹ *ibid* 61.

⁸² Case C-283/81 *CILFIT v Ministero della Sanità* [1982] ECR I-3415, para 16; Case C-220/03 *European Central Bank v Federal Republic of Germany* ECR I-10595, para 31; Lenaerts and Gutiérrez-Fons (n 80) 9.

⁸³ Lenaerts and Gutiérrez-Fons (n 80) 7.

make sense as a whole.⁸⁴ Furthermore, despite its initial drawbacks, the Court has also started to examine the preparatory work of both primary and secondary EU law both as a supplementary interpretative argument, but sometimes also to determine the meaning of a provision in the first place.⁸⁵ In addition, the Court always makes sure that its interpretation is in line with superior legal rules such as the Treaties or the Charter of Fundamental Rights of the EU as well as the Union's objectives.⁸⁶ Lastly, the Court often resorts to teleological interpretation which focuses on the objectives of the legal provision, a method closely linked to the contextual one.⁸⁷

In this case, the Court's statutory interpretation proceeded in a very peculiar fashion. In the quotation above, I have highlighted the key words that provide insights into the Court's approach. The first crucial element is that the Court mentioned that it is not apparent from the wording of the relevant provisions that de-listings should have a global effect. This might point to a higher standard than the usual one.⁸⁸ The meaning of a provision might not be apparent from its wording but it might nevertheless be deducible.⁸⁹ Given the Court's well-established and usual resort to contextual and teleological interpretation, both to form as well as to confirm its findings, it is striking that it chose to restrain itself in considering whether such a meaning was evident exclusively from the text of the law. It seems as if the Court was setting itself up for not finding such meaning in the first place.

The second noteworthy aspect of the Court's analysis is that many words that it used alluded to the intention of the legislator. It is not apparent from the wording of the law that the legislator would have wanted global de-listings, the Court said. Yet it made no effort to discover the legislator's intentions. It did not examine any preparatory work or any other source that would enlighten the thinking behind the relevant provisions,⁹⁰ nor did it even make any particular effort to analyze their text. It simply declared that this was the case. The high bar set by the Court might explain this in part: when the meaning of a provision must be apparent, one could argue that there is no need for much analysis.

The Court was not justified in adopting this approach. First, it did not explain at any point the reason for applying this higher requirement. Perhaps one could argue that I am attaching too much importance to a formulation that is not, after all, unprecedented. However, the lack of any substantial analysis by the Court on this point suggests that a correlation is likely. Second, the Court also did not explain why it did not resort to any sources of legislative intent beyond the text of the GDPR, or any contextual or teleological interpretative methods. After all, this was anything but the typical case cited, where the provision is so clear that it did not warrant further examination. The CJEU has in other cases gone beyond the silence of the legislator using systemic arguments and higher order legal rules.⁹¹ Third, and perhaps most remarkably, the Court confounded the textualist approach with seeking the legislator's intention. I am not aware of any originalist theory that seeks to determine the legislator's intention exclusively from the text, even more so from the apparent meaning of the text.⁹² Hence, the Court's approach was clearly not originalist, nor was it textualist because it did not focus on the meaning of the text but on the intent of the legislators. Even if the Court was adamant in reaching the conclusion it did reach, surely it could have done so with much more methodological rigor.

In the Court's defense, seeking the intention of the legislature in the context of the EU raises particularly hard epistemological problems.⁹³ The EU legislative process is notoriously complex. It involves three parties: the EU Commission that makes a legislative proposal, the Council, in which the governments of the member-states participate, as well as the European Parliament that represents the European people.⁹⁴ The latter two institutions make amendments to the Commission's proposal and have to negotiate to reach agreement. Although neither of them require internal consensus, it is evident that this is a very complex procedure involving a lot of people. Identifying a single intention is challenging. However, the Court did not have to use such an approach. In its jurisprudence it does not more often than it does. And in any case, even if there were no evidence about the legislator's intention, or they were inconclusive, it bore the onus to mention this in its judgment since it took the originalist path,

3.2. Ignoring the elephant in the room: the emphatic absence of the charter of fundamental rights of the EU in the judgment

3.2.1. Can the charter require global takedowns?

Besides the methodological flaws of the Court, there was also a remarkable omission in its judgment. Although the Court acknowledged the possibility that national fundamental rights provisions might require global removal of information, it did

⁸⁴ *ibid* 16–17.

⁸⁵ Despite initial reluctance the Court has slowly started to consider preparatory works in its jurisprudence, see Case C-370/12 *Pringle v Government of Ireland, Ireland and the Attorney General* [2013] 2 CMLR 2, para 135 (2012); Case T-18/10 *Inuit Tapiriit Kanatami v European Parliament* ECR II-5599, para 49; *aff'd* Case C-583/11 P *Inuit Tapiriit Kanatami v European Parliament* [2014] 1 CMLR 54; *Lenaerts and Gutiérrez-Fons* (n 80) 23–32

⁸⁶ Case C-491/10 *Zarraga v Pelz* [2010] ECR I-14247, paras 59–60; Case C-40/11 *Iida v Stadt Ulm* [2013] 1 CMLR 47, para 78. See also *Lenaerts and Gutiérrez-Fons* (n 80) 4.

⁸⁷ *Lenaerts and Gutiérrez-Fons* (n 80) 31–32.

⁸⁸ EU courts have used this term sparingly in the past but it is not clear whether this hints at a deliberate change of standards nor does such an intention seem deducible from the cases in which they used it. See Case C-15/00 *Commission v European Investment Bank (EIB)* [2003] ECR I-07281, para 98; Case T-96/10 *Rutgers Germany GmbH v European Chemicals Agency (ECHA)* 3 CMLR 3, para 107.

⁸⁹ The text of EU data protection law, interpreted in context, could, potentially, lead to a conclusion about its proper reach. See *Bougiakiotis* (n 4) 324–34.

⁹⁰ There is precedent that supports such a practice, see n 85.

⁹¹ See eg Case C-402/07 *Sturgeon v Condor Flugdienst GmbH* [2009] ECR I-10923.

⁹² See generally Keith E Whittington, 'Originalism: A Critical Introduction' (2013) 82 *Fordham L Rev* 375.

⁹³ See generally on indeterminacy and originalism Thomas B McAfee, 'Originalism and Indeterminacy' (1995) 19 *Harv JL & Pub Pol'y* 429; Whittington (n 92) 403; George C Christie, 'The Well-Intentioned Purpose but Weak Epistemological Foundation of Originalism' (2019) 51 *Conn L Rev* 451.

⁹⁴ TFEU, art 294.

not even devote a single line to the question of whether the Charter of Fundamental Rights of the EU could also impose a similar obligation. What is more, the CJEU did not seek to interpret the secondary legislation in light of the Charter, though this is a well-established practice in its case-law.⁹⁵ This omission can have important consequences.

The Charter enshrines both a right to privacy and a right to data protection.⁹⁶ It is true that the level of human rights protection that national law affords will not always coincide with the Charter, even concerning the same rights.⁹⁷ However, it is particularly strange that the fundamental rights to data protection and privacy may mandate global takedowns in national law but this is *never* the case regarding the Charter. This is especially unlikely given that the member states of the EU are also part of the European Convention of Human Rights and Convention 108 of the Council of Europe and share important common principles and traditions.⁹⁸ Hence, at the very least such an effect of the Charter seems worth exploring.

The only argument against issuing global removal orders based on EU rights was in the Advocate General's opinion. He examined the argument of some of the parties that relied on case law of the European Court of Human Rights, which has applied rights extraterritorially. Given that the Charter must offer equal protection to that of the Convention, some litigants called the CJEU to do the same for data protection rights.⁹⁹ However, the Advocate General rejected that argument as incorrect on two grounds. First, he argued, the scope of the CFREU must follow that of the EU and not go beyond it.¹⁰⁰ Second, the Strasbourg case law concerned rights against the death penalty and torture, which are non-derogable, and hence it was not applicable in this case.¹⁰¹

Nevertheless, neither of the Advocate General's arguments are particularly convincing. Regarding the first one, it is true that the Charter follows the scope of EU law. However, as the Advocate General himself admitted, EU law can apply extraterritorially for reasons of effectiveness.¹⁰² Therefore, the real question is not whether the CFREU follows the scope of EU law but whether there are reasons that justify the application of EU data protection law extraterritorially. The Advocate General sought to distinguish between previous cases of extraterritorial application and data protection on the basis that

[t]hose two types of situation [i.e. competition and trade mark law] are in my view extreme situations of an exceptional nature. What is crucial in both situations is the effect on the internal market (even if other markets may also be affected). The internal market is a territory clearly defined

by the Treaties. On the other hand, the internet is by nature worldwide and, in a certain fashion, is present everywhere. It is therefore difficult to draw analogies and make comparisons.¹⁰³

It is not clear though how these situations are so radically different given that they both produce effects inside the EU (which is the crucial parameter per AG Szpunar) and they both have an impact beyond it.¹⁰⁴ In addition, the discussion of cases of trademark and competition law as sufficiently important to warrant extraterritorial application sits oddly with the requirement that a fundamental right be non-derogable to deserve such protection. If reasons of effectiveness justify applying EU laws extraterritorially, surely they should also suffice in the context of the implementation of fundamental rights. The fact that Strasbourg has not applied extraterritorially other, non-absolute, rights does not prevent the CJEU from doing so, nor has the former -to my knowledge- decided upon such a request regarding data protection.

The Advocate General also argued more broadly that global takedowns would make European authorities unable to 'determine a right to receive information, still less to strike a balance between that right and the other fundamental rights to data protection and to private life'.¹⁰⁵ Given that, as he acknowledged, the right to access information in Article 11 of the CFREU concerns only the European public, his argument concerns Europeans living abroad; EU residents are equally affected by geo-blocking measures.¹⁰⁶ The right of foreign citizens to receive information that derives from foreign law is to be accorded less weight as it is merely a foreign interest for the EU. It does seem peculiar that an EU citizen residing abroad will have a right to access information that people residing within the Union do not. However, the Advocate General is right to suggest that legitimate public interest to access information may vary from one-third state to another and hence there is a real problem regarding how to adjust takedown decisions to avoid violating these rights.

Nonetheless, this argument, insofar as it seeks to support the conclusion that EU authorities should not impose any global takedowns, is too far-reaching. It is undoubtedly true that balancing the Article 11 rights of Europeans abroad for all countries in the world is an almost impossible task. The same is true for foreign interests too, since de-listing decisions must take them under consideration as well. Moreover, the Advocate General is right in pointing out that both privacy and access to information rights have equal strength and must be balanced accordingly.¹⁰⁷ Yet, his argument seems to do anything but that. While in some cases access to information could indeed prevail over data protection, arguing that

⁹⁵ *Zarraga* (n 86) paras 59–60; *Iida* (n 86) para 78.

⁹⁶ Charter of Fundamental Rights of the EU, OJ 2010 C 83/389, arts 7–8 (CFREU).

⁹⁷ See eg Case C-399/11 *Melloni v Ministerio Fiscal* EU:C:2013:107 [2013] 2 CMLR 43 where the Spanish constitution provided broader protection than EU law.

⁹⁸ Gloria González Fuster, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Science & Business 2014) chs 3–4.

⁹⁹ *Google v CNIL* AG Opinion (n 49) para 54.

¹⁰⁰ *ibid* para 55.

¹⁰¹ *ibid* para 56.

¹⁰² *ibid.* paras 51–52.

¹⁰³ *ibid.*, para. 53.

¹⁰⁴ This argument essentially sought to support an exceptionalist view regarding Internet regulation. However, it is quite obvious that the Internet can produce effects in the internal market and therefore seeking to distinguish it from other cases on such a basis is unlikely to succeed. The CJEU itself has accepted this see *Google Spain* (n 2) paras 55–56; *Google v CNIL* (n 1) para 57; *Alsenoy and Koekkoek* (n 4) 109.

¹⁰⁵ *Google v CNIL* AG Opinion (n 49) para 60.

¹⁰⁶ *ibid* para 59.

¹⁰⁷ *ibid* para 60.

no takedowns must take place because of difficulties in determining and assessing the parameters of balancing seems to entirely favor access to information.

A case that involves information that is of prevalent public interest to a myriad of countries but not the EU, though theoretically enticing, is marginal at best. Courts and public authorities will, for the most part, be able to identify the countries for which information is important and make the relevant assessment. Moreover, if an interested party disagrees, they can have their say before the competent data protection authority and courts. It is unavoidable that problems will arise in the process. A European decision-maker will not always be in a position to identify if and how information is relevant to a foreign society, its importance may change over time, and parties interested in accessing this information may be unaware of its existence or they may lack the resources to act. It is an imperfect system. However, given that these orders will inescapably infringe some rights, it makes sense to believe that they will cause less harm by depriving some Europeans abroad of some access to information in some marginal cases, than by depriving data subjects of a global remedy entirely.

In any case, this argument is a black and white one. The Advocate General did not explain why this is not a problem when the interests of the EU justify global injunctions on other grounds, despite accepting this as a valid possibility.¹⁰⁸ After all, this already happens in some areas and the Advocate General did not seem to consider it contrary to the Charter. In addition, if imposing global injunctions on the basis of national rights can surpass the hurdle of taking such countervailing rights into account, as the Court clearly thinks, it is difficult to explain why EU authorities will be unable to do so.

3.2.2. *The significance of the charter as a legal basis for global de-referencing*

If the Charter can indeed be a legal basis for global removal orders, this would mean that both EU and national fundamental rights regulate this issue. This has two important consequences. On the one hand, the Charter sets the minimum standards of protection when applying EU law and member states need to abide by them. In other words, the Charter sets the *floor* of protection. On the other hand, the question arises whether member states can exceed its protection and set higher standards, ie whether the Charter is the *ceiling* of protection.

3.2.2.1. *The charter as a floor* Although whether human rights instruments are a ceiling of protection can be controversial both in positive and normative terms, their function as a floor is certain.¹⁰⁹ After all, if a human rights instrument did not set a minimum of protection, its legal significance would be little. This means that member states need to conform to the Charter's requirements when applying EU law. In other

words, member states need to apply data protection law globally, at the very least, in the extent that the Charter requires.

The Court's decision not to discuss the relevant effects of the Charter was a serious omission that might have regrettable consequences. First, it could compromise the rights of EU citizens. Member states will have to make these decisions based on their national human rights law, which means that in some states people can enjoy strong protections, whereas in others, theoretically, none at all.

Second, the Court's elaboration on the global effect of the Charter would have provided member states with a useful yardstick for the implementation of national human rights. Although some could decide to depart from that standard, there would be an implicit onus to consider the necessity of additional protection in relation to the CFREU. Thus, the Charter could have acted as soft harmonisation, providing some coherence to the actions of member states.

Lastly, had the Court addressed this issue, it would enable the legislature to take action in a much clearer landscape. If European lawmakers decide to address this issue, one of the main things they must consider is the protection that the Charter provides.¹¹⁰ If the rules they introduce fall below that bar, they will contravene it, and the CJEU will strike them down. However, as things remain blurry, the potential of them taking such a risky initiative becomes increasingly unlikely.

Of course, this does not mean that this issue is over. Given the weight of the stakes, it is likely that this question will return to Luxembourg for a definitive answer. Perhaps a national court will reject a removal request and the claimant will invoke the Charter, activating the preliminary reference procedure. Perhaps legislators will introduce a provision addressing this issue and someone will dispute its compliance with the Charter. Various scenarios are possible but, in any case, it is probable that the Court will have to elaborate on this issue at some point. However, the Court's insistence on deciding upon data protection cases in the narrowest possible way makes its jurisprudence hydra-like. It resolves one issue and creates two. In doing so, it has put fundamental rights under uncertainty, it has lost the opportunity to prepare the ground for future harmonisation, and it has made the life of legislators more difficult, while creating a need for time and resource consuming, unnecessary litigation.

3.2.2.2. *The Charter as a ceiling* One of the most controversial issues regarding the CFREU is whether it should act as a ceiling for human rights protection. The CJEU has had the opportunity to address this in *Melloni*.¹¹¹ This case concerned the question of whether the member states of the EU can apply national fundamental rights in order to set aside an EU legal provision. Obviously, if member states were able to do so without restriction, they could seriously jeopardize the unity of EU law. The CJEU ruled out this possibility, emphasizing that national fundamental rights cannot be applied in a manner that compromises the 'primacy, unity and effectiveness' of EU law.¹¹² This criterion, however, might be difficult to apply.

¹⁰⁸ See *ibid.*, para. 62 noting that 'I do not exclude the possibility that there may be situations in which the interest of the European Union requires the application of the provisions of Directive 95/46 beyond the territory of the EU'.

¹⁰⁹ CFREU art 53; Federico Fabbrini, *Fundamental Rights in Europe* (OUP 2014) 39.

¹¹⁰ CFREU art 51.

¹¹¹ *Melloni* (n 97).

¹¹² *ibid* para 60.

After all, any application of the member state's fundamental rights is likely to interfere with EU law in this manner.

The Court provided further clarifications on this in the case of *Åklagaren v Fransson*.¹¹³ This case concerned the application of the *ne bis in idem* principle, more usually known as double jeopardy in common law systems. Specifically, Swedish authorities had charged Åkerberg Fransson with tax violations and sought his criminal prosecution. However, before this, they had already imposed administrative sanctions and the question before the Court was whether this would violate the *ne bis in idem* principle. In considering its jurisdiction on the case, the Court noted that when examining whether a provision complies with fundamental rights 'in a situation where action of the Member States is not entirely determined by EU law . . . national authorities and courts remain free to apply national standards'.¹¹⁴

Obviously, the Court relied on this jurisprudence to allow for global injunctions that rely on national fundamental rights. If there is no (secondary) EU law, then national measures cannot compromise its primacy, unity, and effectiveness. However, this holding could undermine the harmonization that the GDPR seeks to effectuate.¹¹⁵ In essence, this criterion distributes power between the legislative and judicial branches. The Court gives the lawmakers the discretion to harmonize further EU law and once they do so, it will intervene to ensure that member-states, based on national human rights do not undercut it.

A question that remains open is what should happen if the action not yet taken by the legislature has underpinnings in primary EU law. Is there a case where national fundamental rights may compromise the unity of EU law without any secondary law provisions at play? This does not seem to be the case at hand. There is, in my view, no legal principle that requires an EU law ceiling on global injunctions. Yet, there are good reasons to introduce one, in some form, to avoid the fragmentation of data protection law in the EU. It is apparent that radically different criteria across EU member states are likely to cause confusion and undercut the harmonisation that is one of the main goals of the GDPR.

4. Conclusion

Google v CNIL is a bit like a rorschach test: it is abstract and confusing enough that what one sees in it probably says more about her than about the judgment. To say that it is open ended would be an understatement. Despite this, there are some important points that can be concluded from it. First, the concerns about the impact of this judgment on international relations are exaggerated. Though a trend of data imperialism might be discernible, the Court was careful enough to avoid infringing foreign sovereignty. Second, the way that the Court went about to reach this very narrow decision was flimsy. This creates more questions for the future, especially regarding the role of the Charter. However, this seems the rule

rather than the exception in the Court's data protection saga. For the time being, both pro-business and pro-privacy speculators can rejoice in the belief that their positions have been vindicated. Their joy, however, might be cut short by the next judgment that is sure to come.

Reference List

'Google Wins Privacy Case' (*New Law Journal*, 25 September 2019) <<https://www.newlawjournal.co.uk/content/google-wins-privacy-case>> accessed 28 December 2020.

Albrecht JP, 'How the GDPR Will Change the World' (2016) 2 EDPL 287.

Alsenoy BV and Koekkoek M, 'Internet and Jurisdiction after Google Spain: The Extraterritorial Reach of the "Right to Be Delisted"' (2015) 5 IDPL 105.

Barlow JP, 'A Declaration of the Independence of Cyberspace' (*Electronic Frontier Foundation*, 8 February 1996) <<https://www.eff.org/cyberspace-independence>> accessed 25 February 2021.

Bougiakiotis E, 'The Enforcement of the Google Spain Ruling' (2016) 24 IJLIT 311.

Bradford A, 'The Brussels Effect' (2012) 107 Nw UL Rev 1.

Bromund TR, 'The U.S. Must Draw a Line on the EU's Data-Protection Imperialism' (*The Heritage Foundation*, 9 January 2018) <<https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism>> accessed 29 January 2021.

Buttarelli G, 'The EU GDPR as a Clarion Call for a New Global Digital Gold Standard' (2016) 6 IDPL 77.

Christie GC, 'The Well-Intentioned Purpose but Weak Epistemological Foundation of Originalism' (2019) 51 Conn L Rev 451.

Clinton WJ and Gore Jr. A, 'A Framework for Global Electronic Commerce' (*The White House*, no date) <<https://clintonwhitehouse4.archives.gov/WH/New/Commerce/read.html>> accessed 21 January 2021.

Cofone I, 'Google v. Spain: A Right to Be Forgotten' (2015) 15 Chi-Kent J Int'l & Comp L 1.

Criscione H, 'Forgetting the Right to Be Forgotten: The Everlasting Negative Implications of a Right to Be Dereferenced on Global Freedom in the Wake of Google v. CNIL' (2020) 32 Pace Int'l L Rev 315.

Endicott T, 'Proportionality and Incommensurability' in G Huscroft, BW Miller, and G Webber (eds), *Proportionality and the Rule of Law: Rights, Justification, Reasoning* (CUP 2014).

European Commission, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation COM (2020) 264 final.

Fabbrini F, *Fundamental Rights in Europe* (OUP 2014).

– and Celeste E, 'The Right to Be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders' (2020) 21 German LJ 55.

Fleisher P, 'Adapting Our Approach to the European Right to Be Forgotten' (*Google- The Keyword*, 4 March 2016) <<https://blog.google/around-the-globe/google-europe/>>

¹¹³ Case C-617/10 *Åklagaren v Fransson* [2013] ECR I-105.

¹¹⁴ *ibid* para 29 (emphasis added).

¹¹⁵ Monika Zalnieriute, 'Google LLC v. Commission Nationale de l'Informatique et Des Libertés (CNIL)' (2020) 114 AJIL 261, 266.

[adapting-our-approach-to-european-rig/>](#) accessed 24 July 2020.

– ‘Three Years of Striking the Right (to Be Forgotten) Balance’ (Google- The Keyword, 15 May 2017) <<https://blog.google/around-the-globe/google-europe/three-years-right-to-be-forgotten-balance/>> accessed 18 December 2020.

Fuster GG, *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Springer Science & Business 2014).

Goldsmith JL, ‘Against Cyberanarchy’ (1998) 65 U Chi L Rev 1199.

– ‘Against Cyberanarchy’ in A Thierer and C Wayne Crews Jr (eds), *Who Rules the Net?: Internet Governance and Jurisdiction* (Cato Institute 2003).

Hertogen A, ‘Letting Lotus Bloom’ (2015) 26 EJIL 901.

Huynh T, ‘Google LLC v. Commission Nationale de l’Informatique et Des Libertés (CNIL): Does Everyone Have to Listen to the European Union?’ (2020) 28 Tul J Int’l & Comp L 359.

ILC, ‘Draft articles on Responsibility of States for Internationally Wrongful Acts’ (2001) UN Doc A/56/10.

Johnson DR and Post D, ‘Law and Borders: The Rise of Law in Cyberspace’ (1996) 48 Stan L Rev 1367.

Kelion L, ‘Google Wins Landmark Right to Be Forgotten Case’, *BBC News* (24 September 2019) <<https://www.bbc.com/news/technology-49808208>> accessed 28 December 2020.

Keller D, ‘Ominous: Canadian Court Orders Google to Remove Search Results Globally’ (*Center for Internet and Society-Stanford Law School*, 28 June 2017) <<http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally>> accessed 27 January 2021.

Kowalik-Bańczyk K and Pollicino O, ‘Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information’ (2016) 17 German LJ 315.

Kozinski A and Goldfoot J, ‘A Declaration of the Dependence of Cyberspace’ (2008–09) 32 Colum JL & Arts 365.

Krotoszynski Jr RJ, ‘Privacy, Remedies and Comity: The Emerging Problem of Global Injunctions and Some Preliminary Thoughts on How Best to Address It’ in A Koltay and P Wragg (eds), *Comparative Privacy and Defamation* (Edward Elgar Publishing 2020).

Kulk S and Borgesius FZ, ‘Google Spain v. Gonzalez: Did the Court Forget about Freedom of Expression’ (2014) 5 Eur J Risk Reg 389.

Kuo MA, ‘The Brussels Effect and China: Shaping Tech Standards’ (*The Diplomat*, 7 January 2020) <<https://thediplomat.com/2021/01/the-brussels-effect-and-china-shaping-tech-standards/>> accessed 27 January 2021.

Lee J-A, Liu C-Y, and Li W, ‘Searching for Internet Freedom in China: A Case Study on Google’s China Experience’ (2013) 31 Cardozo Arts & Ent LJ 405.

Lenaerts K and Gutiérrez-Fons JA, ‘To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice’ (2013) 20 Colum J Eur L 3.

Lowe AV, ‘Blocking Extraterritorial Jurisdiction: The British Protection of Trading Interests Act, 1980’ (1981) 75 AJIL 257.

Lynskey O, ‘Control over Personal Data in a Digital Age: Google Spain v AEPD and Mario Costeja Gonzalez’ (2015) 78 MLR 522.

– ‘Extraterritorial Impact in Data Protection Law through an EU Law Lens’ (2020) Brexit Institute Working Paper Series No 8/2020 <<https://papers.ssrn.com/abstract=3674413>> accessed 6 August 2021.

Ma A, ‘Russia Officially Introduced a “Sovereign Internet” Law to Let Putin Cut Off the Entire Country from the Rest of the Web’ (*Business Insider*, 1 November 2019) <<https://www.businessinsider.com/russia-sovereign-internet-law-cut-web-access-censorship-2019-11>> accessed 26 February 2021.

Mann FA, *The Doctrine of Jurisdiction in International Law* (AW Sijthoff 1964).

Mannion C, ‘Data Imperialism: The GDPR’s Disastrous Impact on Africa’s E-Commerce Markets’ (2020) 53 Vand J Transnat’l L 685.

Mantelero A, ‘The Future of Data Protection: Gold Standard vs. Global Standard’ (2021) 40 CLS Rev 105500.

Marinett M, ‘The Race to the Bottom: Comity and Cooperation in Global Internet Takedown Orders’ (2020) 53 UBCL Rev 463.

McAffee TB, ‘Originalism and Indeterminacy’ (1995) 19 Harv JL & Pub Pol’y 429.

Minora LE, ‘US Courts Should Not Let Europe’s Right to Be Forgotten Force the World to Forget’ (2017) 89 Temp L Rev 609.

Nunziato DC, ‘The Fourth Year of Forgetting: The Troubling Expansion of the Right to Be Forgotten’ (2018) 39 U Pa J Int’l L 1011.

Raz J, *Practical Reason and Norms* (OUP 1999).

Rustad ML and Koenig TH, ‘Towards a Global Data Privacy Standard’ (2019) 71 Fla L Rev 365.

Ryngaert C, *Jurisdiction in International Law* (2nd edn, OUP 2015).

Satariano A, ‘G.D.P.R., a New Privacy Law, Makes Europe World’s Leading Tech Watchdog’, *The New York Times* (24 May 2018) <<https://www.nytimes.com/2018/05/24/technology/europe-gdpr-privacy.html>> accessed 8 July 2020.

Schultz T, ‘Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface’ (2008) 19 EJIL 799.

Schwartz PM, ‘Global Data Privacy: The EU Way’ (2019) 94 NYUL Rev 771.

– ‘The EU-US Privacy Collision: A Turn to Institutions and Procedures’ (2013) 126 Harvard L Rev 1966.

Scott M and Cerulus L, ‘Europe’s New Data Protection Rules Export Privacy Standards Worldwide’ (POLITICO, 31 January 2018) <<https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/>> accessed 21 January 2021.

– ‘Russia and China Push “Fake News” Aimed at Weakening Europe: Report’ (Politico, 1 April 2020) <<https://www.politico.eu/article/russia-china-disinformation-coronavirus-covid19-facebook-google/>> accessed 15 July 2020.

Tiezzi S, ‘China’s “Sovereign Internet”’ (*The Diplomat*, 24 June 2014) <<https://thediplomat.com/2014/06/chinas-sovereign-internet/>> accessed 26 February 2021.

Tsakyrakis S, ‘Proportionality: An Assault on Human Rights?’ (2009) 7 ICON 468.

United States Department Of State, ‘Global Internet Freedom Task Force’ (Department Of State, The Office of Electronic Information, Bureau of Public Affairs 2001–09) <<https://www.state.gov/e/oe/b/ia/>>

[//2001-2009.state.gov/g/drl/lbr/c26696.htm](https://2001-2009.state.gov/g/drl/lbr/c26696.htm)> accessed 21 January 2021.

Whittington KE, 'Originalism: A Critical Introduction' (2013) 82 Fordham L Rev 375.

Woods AK, 'Against Data Exceptionalism' (2016) 68 Stan L Rev 729.

– 'Litigating Data Sovereignty' (2018) 128 Yale LJ 328.

Zalnieriute M, 'Google LLC v. Commission Nationale de l'informatique et Des Libertés (CNIL)' (2020) 114 AJIL 261.

Zittrain J, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' in A Thierer and CW Crews Jr. (eds), *Who Rules the Net?: Internet Governance and Jurisdiction* (Cato Institute 2003).

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

Acknowledgements

Many thanks to Tatiana Cutts and Dimitra Louizidi for their valuable comments. The usual disclaimer applies.