

Reasonableness in its reasoning: How the European Union can mitigate problematic extraterritoriality on a de-territorialised internet

*Mistale Taylor**

1. Introduction

There is an extraterritorial character to European Union (EU) data protection law that can be both necessary and problematic.¹ EU lawmakers are enacting regulation that directly or indirectly compels non-EU (third State) actors to behave in a particular way to comply with EU law. In contrast to many of these third countries, numerous instruments and jurisprudence all affirm the fundamental right to data protection's increasingly lofty status in the EU.² Characterising data protection as a fundamental right bestows an obligation upon the EU to guarantee its data subjects' right to have their personal data kept private and safe. These data subjects are usually EU residents or, at least, present on its territory. This protective obligation entails safeguarding EU data subjects' right to data protection against extraterritorial or third State violations in specific, limited circumstances. It is, however, important to keep these circumstances limited when the EU prescribes the law or, in other words, exercises prescriptive jurisdiction extraterritorially. One such important restraining device is the concept of jurisdictional reasonableness.

* Senior Research Analyst at Trilateral Research and Counsel at Public International Law and Policy Group.

¹ See, *inter alia*, D Jerker, B Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing 2013); B Van Alsenoy, 'Reconciling the (extra)territorial Reach of the GDPR with Public International Law' in G Vermeulen, E Lievens (eds), *Data Protection and Privacy Under Pressure. Transatlantic Tensions, EU Surveillance and Big Data* (Maklu 2017).

² Eg European Union, Consolidated version of the Treaty on the Functioning of the European Union (13 December 2007) 2008/C 115/01, art 16(1); Charter of Fundamental Rights of the European Union [2010] OJ C 83/02, art 8.



EU data protection laws with extraterritorial effect can be fit into traditional permissive principles of jurisdiction under public international law. Principles based on where an act is initiated or culminated (subjective territoriality, objective territoriality), the nationality of the victim (passive personality) or where a detrimental effect is felt (effects doctrine) could all be applicable in this context. Simply being applicable, however, could permit the EU's data protection laws to extend too far; it might not allow for States with stronger jurisdictional claims to regulate a situation. As an authoritative, well-established legal framework, the public international law of jurisdiction could provide guidance on how to solve conflicts in terms of sovereignty. That is not to neglect the unhelpful capaciousness of various jurisdictional principles and, indeed, the conflicts that the traditional laws on jurisdiction have caused. It would also not effectively solve all the present issues, particularly with regard to fundamental rights. As such, a so-called second-tier, additional set of criteria needs to be considered in such situations to restrain jurisdictional overreach, thus mitigating conflicts and tensions.

Jurisdictional overreach should be mitigated when it causes tensions by encroaching upon foreign State sovereignty. That said, overreach that causes international tension is problematic, but sometimes overreach (tension-causing or not) is necessary for rights protection. This second-tier set of criteria includes establishing a connection between the regulation and the regulated beyond the aforementioned territoriality/nationality principles, and interest-balancing under the rubric of reasonableness. These concepts are not mutually exclusive and consistently overlap, but this contribution limits itself to reasonableness as it appears in the Third and, to a lesser degree, the Fourth Restatement of US Foreign Relations Law.³ These Restatements outline the US approach to foreign relations law and international law as it applies to the US, and include authoritative sections on, *inter alia*, jurisdiction.⁴ These sections have influenced scholarship, non-US courts and international conceptions of how States should exercise jurisdiction. This contribution outlines a rule of reason useful for the data protection legal sphere. It then examines the

³ *Restatement (Third) of the Foreign Relations Law of the United States* (Am Law Inst 1987); *Restatement (Fourth) of the Foreign Relations Law of the United States* (Am Law Inst 2018).

⁴ See <www.ali.org/publications/show/foreign-relations-law-united-states/>.



application of reasonableness in a recent judgement of the Court of Justice of the European Union (CJEU), *Google Inc v Commission nationale de l'informatique et des libertés (CNIL) (Google v CNIL)*, which has potentially far-reaching consequences.⁵ Taken together with other means for assessing when a State may regulate a situation, reasonableness is both useful and important.

2. *Data protection jurisdiction in the internet age*

Most data processing happens in the virtual, online sphere. The advent of the internet challenges traditional approaches to jurisdiction, which are rooted in territory. As such, not only do the traditional, first-tier permissive principles mentioned in the foregoing section, but also the second-tier mitigating factors need to be re-examined in view of these technological developments. On jurisdiction in the internet age, Dan Jerker B. Svantesson has proposed a three-pronged test combining connection, interest and reasonableness considerations.⁶ He does away with the first-tier permissive principles that revolve around territoriality and personality, and instead moves straight to the second-tier principles usually used to assess the lawfulness of the assertion of jurisdiction after a permissive principle is established. He bases these mostly on the seminal 1935 Harvard Research Draft Convention on Jurisdiction with Respect to Crime, and reinterprets them in view of how the internet challenges existing notions of territory-based jurisdiction:⁷

'In the absence of an obligation under international law to exercise jurisdiction, a state may only exercise jurisdiction where:

- (1) there is a substantial connection between the matter and the state seeking to exercise jurisdiction;
- (2) the state seeking to exercise jurisdiction has a legitimate interest in the matter; and

⁵ Case C-505/17 *Google Inc v Commission nationale de l'informatique et des libertés (CNIL)* (24 September 2019).

⁶ D Jerker, B Svantesson, 'A New Jurisprudential Framework for Jurisdiction' (2015) 109 *AJIL Unbound* 69, 74.

⁷ 'Draft Convention on Jurisdiction with Respect to Crime' (1935) 29 *AJIL Supplement: Research in International Law* 439, 439-442.



(3) the exercise of jurisdiction is reasonable given the balance between the state's legitimate interests and other interests'.⁸

Both he and respondents to his suggestion confirm this is not novel; rather he is bringing the three ideas together and suggesting they could apply effectively in the complex data protection world with malleable borders and differing interests.⁹ Svantesson's test applies 'in the absence of an obligation under international law to exercise jurisdiction [...]'.¹⁰ According to some interpretations of international human rights law and EU law, the EU could be understood to have an *obligation* to protect its data subjects' fundamental rights in certain extraterritorial situations.¹¹ If so, there would be no 'absence of an obligation' needed to apply Svantesson's criteria. The EU's obligation, however, is not absolute or always applicable. If this obligation were not clearly palpable or needed some limit, a version of the above criteria could be applied. The subsequent sections assume the EU's obligations to exercise jurisdiction are not absolute and thus warrant a traditional basis of jurisdiction and restraining devices to be considered legitimate and effective. It focuses on reasonableness as such a restraining device.

2. Reasonableness

The EU's exercise of jurisdiction ought to be reasonable. To assess reasonableness, as a subset of comity (discussed below), various interests need to be balanced. This section explains the notion of interest before discussing it in the context of comity and, more specifically, interest-balancing. Interest-balancing in the data protection sphere is linked closely

⁸ D Jerker, B Svantesson, *Solving the Internet Jurisdiction Puzzle* (OUP 2017) 61 (as first unveiled in Svantesson (n 6) 74).

⁹ Eg C Ryngaert, 'Old Wine into New Bottles – Comment on "A New Jurisprudential Framework for Jurisdiction"' (2015) 109 *AJIL Unbound* 81.

¹⁰ Svantesson (n 6).

¹¹ See generally L Bartels, 'The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects' (2015) 25 *EJIL* 1071, 1078 and, on the right to privacy (connoted with the right to data protection), M Milanovic, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' (2015) 56 *Harvard Intl LJ* 81.



to individuals and their rights. The section ends by outlining a rule of reason, which itself is intertwined with the aforementioned concepts.

2.1. *Comity*

Comity is a non-legally binding principle whereby States conduct relations, including exercising jurisdiction, by *inter alia* taking into account other States' interests, citizens' rights, duties and practicality in a spirit of courteousness, respect and deference.¹² The concept is multi-faceted and broad, and spans multiple disciplines including private and public international law.¹³ It is closely linked to reasonableness. Some scholars suggest reasonableness and comity are interchangeable; others suggest the rule of reason falls within the notion of comity.¹⁴ Comity is understood as an underlying principle in law, international relations and other disciplines, and reasonableness is a rule enshrined in specific legal sources, which makes more specific demands to act reasonably than does the general doctrine of comity.

Comity is not without criticism. In antitrust law in particular, US courts have not understood comity as authoritatively commanding their consideration of external interests.¹⁵ Accordingly, comity in that example foregrounds domestic concerns over international ones.¹⁶ It suffers from being insular. Scholars have therefore criticised comity as manifested in the Third Restatement as not accurately reflecting how US courts apply the law.¹⁷ Rather, they suggest it is a rule to aspire to. As comity is such a nebulous concept, it has been condemned as providing little legal certainty and predictability.¹⁸ This research nonetheless considers comity as a principle underlying reasonableness. This background helps inform the reasonableness assessment of the CJEU case discussed below. Comity is related to interest-balancing, which forms part of this assessment.

¹² See eg *Black's Law Dictionary* (6th edn, West Publishing Co 1990) 267.

¹³ JR Paul, 'The Transformation of International Comity' (2008) 71 *L Contemporary Problems* 19, 19-20 (citations omitted).

¹⁴ *ibid* 4, fn 20 (citations omitted).

¹⁵ HL Buxbaum, 'Territory, Territoriality and the Resolution of Jurisdictional Conflicts' (2009) 57(2) *American J Comparative L* 631, 649 (citations omitted).

¹⁶ *ibid*.

¹⁷ *ibid*.

¹⁸ C Ryngaert, *Jurisdiction in International Law* (2nd edn, OUP 2015) 172.



2.2. *The enduring appeal of the Third Restatement of US Foreign Relations Law*

The 1987 Third Restatement of US Foreign Relations Law controversially introduced a section on jurisdictional ‘reasonableness’, which asserted that customary international law required US courts to decide, on a case-by-case basis, whether applying domestic law in cases with a foreign element was reasonable.¹⁹ It outlined an interest-balancing test.²⁰ The 2018 Fourth Restatement that replaces it, however, has eliminated this section. Whilst it still reflects principles of reasonableness and doctrines of international comity, these principles and doctrines allow less case-by-case discretion by courts. Indeed, William Dodge, a drafter of the Fourth Restatement, claims that reasonableness is decidedly not absent and is instead manifested in the Fourth Restatement’s provisions on the presumption against extraterritoriality and reasonableness in statutory interpretation.²¹ Indeed, the Fourth Restatement ‘has not abandoned reasonableness’.²²

This contribution takes inspiration from reasonableness and interest-balancing as anchored in the Third Restatement. It uses the terminology of both Restatements, but does not use them *per se* as a legal basis for its assessment. Whilst the Fourth Restatement reframes reasonableness from a US perspective, the principle itself is present in international law, but does not yet amount to customary international law. Notions of reasonableness are found in comity principles. This research thus assimilates the Third and Fourth Restatements of US Foreign Relations Law and focuses largely on the Third Restatement’s discourse on reasonableness and interest-balancing and, from this, derives a rule of reason unique to extraterritorial jurisdiction in the data protection sphere.

2.3. *Interest*

In demarcating a State’s exercise of prescriptive jurisdiction over a situation with links to another State, the EU ought to consider sovereign,

¹⁹ Third Restatement § 403.

²⁰ *ibid.*

²¹ WS Dodge, Reasonableness in the Restatement (Fourth) of Foreign Relations Law (2019) 54 *Willamette L R* (forthcoming) available at <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3373370> 2, citing Fourth Restatement §§ 404 and 405.

²² *ibid.* 19.



individual and global interests. Firstly, in a discussion on far-reaching claims of jurisdiction, sovereign interests are important. Secondly, the EU wants to protect its residents who are data subjects. EU data protection law with extraterritorial effect focuses on protecting individuals rather than the EU itself or Member States. Its human rights dimension revolves around protecting individual interests. International and regional instruments recognise the rights to privacy and data protection, which could connote extraterritorial obligations to ensure full and effective protection of an individual concerning activities played out in a virtual space, so individual interests should be taken into consideration. Thirdly, global interests are important because of the worldwide reach of the internet: online data processing can affect people in many jurisdictions. Influential data protection laws such as the EU's could have benefits for the international community as a whole.

2.3.1. *Interest-balancing*

The concept of interest-balancing as a second-tier approach to jurisdictional issues, along with substantial connection and legitimate interest, emerged in US antitrust law in the 1970s.²³ In situations where two State's jurisdictional assertions conflict, each one is obliged 'to evaluate its own as well as the other state's interest in exercising jurisdiction [whereafter] a state should defer to the other state if that state's interest is clearly greater'.²⁴ Much scholarship also supports the concept of weighing up interests and attempting to balance these interests to mitigate jurisdictional conflicts.²⁵

Questions have been raised, however, as to whether interest-balancing can or should be realised. It has been suggested that its 1970s and 1980s glory days were limited.²⁶ Courts, States and scholars have

²³ Buxbaum (n 15) 646 citing *Timberlane Lumber Co. v Bank of America*, N.T., 549 F.2d 597, 609 (C.A. Cal. 1976).

²⁴ Third Restatement § 403 (3).

²⁵ See, eg K Meessen, 'Antitrust Jurisdiction under Customary International Law' in Buxbaum (n 15) 657 citing KM Meessen, *Völkerrechtliche Grundsätze des internationalen Kartellrechts* (Nomos Verlagsgesellschaft 1975) 182.

²⁶ Buxbaum (n 15) 650; on Svantesson's proposed three-pronged test (see below), Muir Watt questions the potentially retrograde interest-balancing prong: 'a return to familiar forms of state interest analysis is not necessarily the best way to go about [overhauling the concept of extraterritorial sovereignty]'. H Muir Watt, 'A Private

exhibited skepticism at the concept, often rejecting it as being unworkable in practice. European States have been ‘generally uneasy’ at using interest balancing to solve jurisdictional conflicts.²⁷ In line with the view of some courts, the mere act of considering foreign interests could be understood not as a public international law mandate, but more an exercise in international relations.²⁸ Francis A. Mann in 1984 suggested that beyond the US, there was no support for the theory of interest-balancing in traditional public international law sources and that it ought to be firmly rejected.²⁹ Indeed, what constitutes ‘interests’ is politicised and broad, and does not lend itself to a true, predictable legal measure that could effectively lessen conflicts in jurisdiction or solve those that have arisen. That said, interest-balancing is not nearly irrelevant when looking at jurisdictional conflicts in the data protection sphere.

Interest-balancing is useful, but also challenging, precisely because there are so many stakeholders and interests to be balanced in the online privacy sphere. As data protection has, since the early 1980s, evolved from an economic necessity to a human right, interest-balancing can be conceived of in human rights terms. Data protection is enshrined as a fundamental right in the EU Charter of Fundamental Rights (EU Charter), thus sometimes implying extraterritorial obligations, which further strengthens the impetus to focus on interests in terms of individual rights.³⁰ This does not mean, however, that the interests of the US or others should be excluded; rather, the interest-balancing test takes on a different character in this context, as explained below.

(International) Law Perspective - Comment on “A New Jurisprudential Framework for Jurisdiction” (2017) 109 *AJIL* Unbound 75, 79.

²⁷ Ryngaert (n 18) 171.

²⁸ Buxbaum (n 15) 656 (citations omitted).

²⁹ Ryngaert (n 18) 153 citing FA Mann, *The Doctrine of Jurisdiction in International Law* (AW Sijthoff 1964) 20.

³⁰ There is no jurisdictional clause as such in the EU Charter. It applies when EU Member States are implementing EU law, which could stretch beyond the geographical scope of the Union (V Moreno-Lax, C Costello, ‘The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territoriality to Facticity, the Effectiveness Model’ in S Peers, T Hervey, J Kenner, A Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (Hart Publishing 2014) 1658). Another approach is to consider certain important human rights treaties, charters or documents as applying extraterritorially in specific situations (see M Milanovic, *Extraterritorial Application of Human Rights Treaties: Law, Principles, and Policy* (OUP 2011) 263).



2.3.2. *Balancing rights*

A human rights-focused approach is important when using interest-balancing to assess the legitimacy of extraterritorial jurisdictional claims as they pertain to rights realised online. It is important to balance the right to data protection with other imperatives, such as objectives of the general (global) interest, and the rights of others. As illustrated by the interest-balancing approaches outlined *supra*, courts have attempted to balance conflicting legal and policy considerations to resolve tensions in jurisdiction.³¹ As almost all legal issues today can be framed as a question of human rights, and are increasingly framed as such, an international human rights law approach is relevant.

The right to privacy and personal data protection, both being fundamental freedoms, are non-absolute and derogable, and may be limited. In general international human rights law, derogations must be prescribed by law, fulfil a certain objective, and be necessary and proportionate. Specifically, the European Convention of Human Rights (ECHR), to which all EU Member States are party, provides in Article 8 on the right to privacy, which includes a right to data protection, that a public authority may interfere in this right only if that interference is ‘in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others’.³² Similarly, the EU Charter provides that limitations on exercising any rights it recognises must fulfil the following criteria:

‘[Any limitation] must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others’.³³

³¹ Muir Watt (n 26) 77; A Mills, ‘Rethinking Jurisdiction in International Law’ (2014) 84 *British YB Intl L* 187, 233.

³² ECHR art 8(2).

³³ EU Charter art 52(1).

Whilst a full assessment of the extent to which certain competing rights may be limited or derogated from is beyond the scope of this research, it is useful to recall that States may limit certain rights whilst respecting their ‘essence’.³⁴ As an approach to extraterritorial jurisdiction in cases concerning data protection, a rule of reason is useful for legislators and courts.

2.3.3. *Reasonableness and a rule of reason*

The concept of ‘interest-balancing’ can be linked directly to reasonableness.³⁵ Reasonableness is a key mitigating factor when considering the extraterritoriality of the EU’s jurisdictional assertions. The Third Restatement of US Foreign Relations Law provides that where a State seeks to exercise prescriptive jurisdiction over a situation with foreign elements, the traditional bases for exercising jurisdiction (territoriality, nationality and similar) in themselves are not enough to justify exercising jurisdiction.³⁶ A State must refrain from exercising jurisdiction based on one of those principles when this exercise is unreasonable.³⁷ The conceptual basis of this reasonableness provision is that a State ‘with the weaker interest ought to defer to the State with the stronger interest’.³⁸ As a factor to consider when assessing unreasonableness, the Third Restatement includes, amongst several others, another State’s interest in regulating the matter at hand.³⁹ If unreasonableness were established, this would mean a State may not exercise jurisdiction even if, for instance, it had established a territorial link to a situation. However, if two States exercised jurisdiction with reason, but what they prescribed was conflicting, each State would be obliged to balance interests, deferring to that with the

³⁴ M Brkan, ‘The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way Through the Maze of the CJEU’s Constitutional Reasoning’ (2019) 20 *German L J* 864, 869.

³⁵ HG Maier, ‘Interest Balancing and Extraterritorial Jurisdiction’ (1983) 31 *American J Comparative L* 579, 589 citing JR Atwood, K Brewster, *Antitrust and American Business Abroad* (2d ed, Shephard’s/Mc Graw Hill 1981) 173-78.

³⁶ Third Restatement § 403(1).

³⁷ *ibid* § 403(1).

³⁸ Ryngaert (n 18) 172.

³⁹ Third Restatement § 403(2)(g).



greater interest.⁴⁰ This appears to foreground interest-balancing when resolving a conflict of jurisdiction in an international setting. At the same time, the Third Restatement includes interest considerations along with several other factors, such as the character of the regulated activity and the likelihood of conflict, when determining the reasonableness and thus eventual legitimacy of an assertion of jurisdiction. The drafters of the Third Restatement have shown they conceived of the reasonableness principle as a rule of (public) international law, albeit with roots in private international law methodology.⁴¹ Some have affirmed this position in understanding reasonableness to be a customary international law rule, but this has been rejected in the Fourth Restatement of US Foreign Relations Law.⁴²

That said, reasonableness has suffered similar criticism to comity, outlined above. Courts could use ‘reasonableness’, masquerading as an international jurisdictional rule of reason, in place of analysis.⁴³ In light with that sentiment, reasonableness has been condemned as a vehicle to promote domestic US interests abroad.⁴⁴ Most of these criticisms – and those applied to comity – could be transplanted onto the EU’s expansionist attitude to data protection law jurisdiction. Nonetheless, establishing a degree of connection and interest-balancing are relevant and useful in assessing the legitimacy of the EU’s exercise of extraterritorial jurisdiction in the internet age, which throws traditional concepts of territoriality into question. Flowing from this, a specific rule of reason materialises. A State may legitimately exercise jurisdiction based on a permissive principle exercised reasonably, that is, after regulators have balanced different interests and rights to identify the State with the strongest interest in regulating the situation. In part due to the worldwide reach of the internet, the global interest should not be harmed.

⁴⁰ *ibid* § 403(3); cf too the ‘view that a court should not exercise comity if doing so would be contrary to its own nation’s interests or policies’. SA Kadish, ‘Comity and the International Application of the Sherman Act: Encouraging the Courts to Enter the Political Arena’ (1982) 4(1) *Northwestern J Intl L & Business* 130, 133.

⁴¹ Buxbaum (n 15) 648 (citations omitted).

⁴² *ibid* 649 citing Frederick Alexander Mann, *The Doctrine of Jurisdiction in International Law* (AW Sijthoff 1964) 9-116.

⁴³ This was asserted in reference to US courts. Maier (n 35) 590 (citations omitted).

⁴⁴ *ibid* 590 (citations omitted).

3. *Applying reasonableness*

This section examines how the CJEU did or did not apply reasonableness when assessing the territorial reach of the right to erasure or ‘right to be forgotten’ in *Google v CNIL*.⁴⁵ It also touches briefly upon a CJEU case (*Eva Glawischnig-Piesczek v Facebook Ireland*) about the territorial reach of content blocking on social media platforms.⁴⁶ Returning to the former, EU residents may request that Google remove links to websites with certain information about them from its search results.⁴⁷ The territorial question involves Google users outside the EU seeing search results with these links removed. In terms of jurisdiction, the Court’s pronouncements on how far EU Member State law may extend beyond EU borders is important regarding how each State prescribes and defines the reach of the law. As the Court stipulates, authorities within each State have the competence to make those assessments in terms of the right to erasure.⁴⁸ The CJEU was deciding whether there was a close enough connection and properly balanced interests for the EU ultimately to regulate a situation occurring outside the EU. It did so in an eminently reasonable manner, especially in view of related provisions in the Third Restatement. It did not, however, completely exclude the extraterritorial application of EU data protection law and it left a large interest- and rights-balancing role to the independent data protection supervisory authorities in Member States.

3.1. *Proceedings in France and at the Court of Justice of the European Union*

In a landmark CJEU decision in 2014 involving a Spanish individual and Google, the Court ruled that the individual had a right to erasure or ‘right to be forgotten’.⁴⁹ This meant that Google as a search engine operator was obliged to de-reference results pertaining to an individual who

⁴⁵ *Google v CNIL* (n 5).

⁴⁶ Case C-18/18 *Eva Glawischnig-Piesczek v. Facebook Ireland Limited* (3 October 2019).

⁴⁷ Case C-131/12 *Google Spain v AEPD and Mario Costeja Gonzalez* (Grand Chamber 13 May 2014) para 94.

⁴⁸ *Google v CNIL* (n 5) 72.

⁴⁹ *Google Spain* (n 47).



had requested this removal, if it deemed the results inaccurate, inadequate, irrelevant, excessive or outdated.⁵⁰ In balancing interests and rights, the Court stated that, in most situations, an individual's rights to privacy and data protection 'override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name'.⁵¹ This paved the way for the Court to favour an individual's data protection interests and rights over other, competing interests. The right to erasure is now enshrined in the GDPR.⁵² Google initially implemented the judgement to affect the search results of users accessing the local version of Google (meaning google.fr in France, but not google.com in France). The French Data Protection Authority (*Commission nationale de l'informatique et des libertés* or CNIL), which is an independent supervisor of how EU data protection law is implemented and adhered to, ordered Google to apply the right to all versions of Google accessed from everywhere. Google then implemented the right so that most users in the EU would, broadly, see redacted results no matter which version of Google they used (google.fr, google.com.au and so on).⁵³ CNIL then fined Google 100,000 EUR for not delisting results from all versions of Google.⁵⁴ Eventually, the matter came before the Grand Chamber of the CJEU, which was to decide on the implementation of EU law. The CJEU had to determine the required territorial scope of the dereferencing in such a situation.⁵⁵ It had to assess whether EU law obliged the search engine operator to remove results within only one relevant Member State, within the whole EU or globally.

The Court concluded that a search engine operator (Google) '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'.⁵⁶ This means that there is no obligation in EU law for

⁵⁰ *ibid* 94.

⁵¹ *ibid* 99.

⁵² GDPR art 17.

⁵³ Users in the country of the 'de-referenced' data subject would see redacted results on all versions of Google; EU-based users not in that country would see redacted results on EU Google domains.

⁵⁴ J Fioretti, 'France fines Google over "right to be forgotten"' (24 March 2016) available at <www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX>.

⁵⁵ *Google v CNIL* (n 5) para 53.

⁵⁶ *ibid* 74.

the search engine operator to dereference results globally, so that any version of Google accessed anywhere in the world would show a redacted list of results.⁵⁷ This is, however, not prohibited.⁵⁸ The dereferencing may not occur in only the one Member State where the requesting individual resides, but is ‘in principle, supposed to be carried out in respect of all the Member States’.⁵⁹ The search engine operator must, where necessary ‘effectively prevent or, at the very least, seriously discourage’ a user from accessing the links that a data subject initially asked the search engine operator to delist.⁶⁰ The following section analyses the Court’s reasoning and decision in the *Google v CNIL* case in view of the reasonableness aspect of the rule of reason outlined above.

3.2. *Reasonableness in its reasoning*

Whereas the provision on extraterritorial jurisdiction in the Third Restatement of US Foreign Relations Law had not been embraced by the US Supreme Court or the CJEU, the *Google v CNIL* judgement nevertheless exemplifies the Court conducting an interest- and rights-balancing exercise.⁶¹ The Court makes connections between regulations and the regulated, which were centred on territory, but it also considers various interests when determining the reach of the EU manifestation of the right to erasure.⁶²

In such a case, it is important to consider connections beyond pure territory, such as nationality or economic activity, between the regulating State or authority (the EU) and those the regulation is designed to protect.⁶³ Although the GDPR states that that ‘protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data’, the Regulation ordinarily applies to EU data subjects who are usually residents of an EU Member State.⁶⁴ Indeed, such a broad scope of

⁵⁷ *ibid.*

⁵⁸ *ibid* 72.

⁵⁹ *ibid* 66.

⁶⁰ *ibid* 74.

⁶¹ Dodge (n 21).

⁶² *Google v CNIL* (n 5) para 52.

⁶³ See eg Third Restatement § 403 (2)(b).

⁶⁴ GDPR recitals 2 and 14.



application implied in that provision in the GDPR would be unacceptable under public international law, not to mention it being unwieldy and unenforceable in practice. As such, in the present case, the necessary connection between the EU and EU data subjects is fulfilled. Beyond that, however, the Court does not attempt to require the application of this law to those outside Union territory: '[i]t is in no way apparent from the wording of [provisions on the right to erasure] that the EU legislature would, for the purposes of [guaranteeing a high level of protection of personal data throughout the EU], have chosen to confer a scope on the rights enshrined in those provisions which would go beyond the territory of the Member States'.⁶⁵ The Court thus recognises that EU lawmakers did not explicitly intend for the universal application of the right to erasure. Furthermore, if an internet user who is either in the EU or outside the EU accessed a link regarding 'a person whose centre of interests is situated in the Union', this would likely 'have immediate and substantial effects on that person *within the Union itself*'.⁶⁶ Again, the protected individual has his or her 'centre of interests' in the EU and feels the effect of the regulation in the EU; there exists some sort of a connection to the EU. The Court uses this notion of territorial effects to imply that global de-referencing would not be unlawful, indeed it could be necessary to prevent harmful effects within the EU.⁶⁷ As such, the Court successfully moves beyond pure territoriality to consider where effects are felt (not where the whole conduct takes place) and territorial connections (EU data subject and search engine user in the EU).

Beyond the individual, the Court ought to consider another State's interest in regulating the activity.⁶⁸ In the present example, this other State would be a non-EU State. Evidently, that State would have an interest in regulating the version of Google its users see. Even if their residents may not enjoy EU data protection rights, if they are subject to the effects of EU data protection legislation, non-EU States would have such an interest in regulating the activity. In this assessment, the Court should

⁶⁵ *Google v CNIL* (n 5) para 62 citing para 54.

⁶⁶ *ibid* 52 (emphasis added).

⁶⁷ *ibid* 58.

⁶⁸ See eg Third Restatement § 403 (2)(g).



consider the nature of the regulated activity (being an EU-centric right to erasure) and how much other States regulate this activity.⁶⁹

According to this contribution's unique rule of reason, interest-balancing is intertwined with rights-balancing. To that effect, the CJEU notes that both the pre-2018 Data Protection Directive (DPD) and the GDPR were adopted on the basis of Article 16 of the Treaty on the Functioning of the European Union, which prescribes that everyone has the right to the protection of his or her personal data.⁷⁰ As such, their objectives are to 'to guarantee a high level of protection of personal data throughout the European Union'.⁷¹ The Court acknowledges that global dereferencing would 'meet that objective in full'.⁷² It then, however, stops itself from extending the reach of EU law too far by considering the interests of other States in emphasising that numerous third States do not recognise a right to erasure or have a different approach thereto.⁷³ The Court also acknowledges that the right to data protection is not absolute and should be balanced against other fundamental rights.⁷⁴ These rights, which are likely to 'vary significantly' around the world include the rights to privacy and data protection balanced with the freedom of information for internet users.⁷⁵ As such, without going so far as conducting a full rights-balancing exercise itself, the Court reasonably ascertains that EU rights conceptions ought not to extend unilaterally into third State jurisdictions, which have different conceptions of these same rights.

Interestingly, the CJEU refers to this difference even within the EU itself. It mentions the public's interest in accessing information and that 'weighing up that interest, on the one hand, and a data subject's rights to privacy and the protection of personal data, on the other' could differ

⁶⁹ *ibid* § 403 (2)(c); a summary of other States' conceptions of the right to erasure enshrined in law is available here: D Erdos, K Garstka, 'The "Right to be Forgotten" Online within G20 Statutory Data Protection Frameworks' (2019) available at <<https://ssrn.com/abstract=3451269>>.

⁷⁰ *Google v CNIL* (n 5) para 54 citing TFEU art 16; 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 [1995] OJ 1995 L 281/31.

⁷¹ *ibid*.

⁷² *ibid* 55.

⁷³ *ibid* 59.

⁷⁴ *ibid* 60.

⁷⁵ *ibid*.



between Member States.⁷⁶ It urges cooperation between national data protection authorities to achieve coherence. The Court considers that the EU legislature has struck such a balance within the EU, but has not found this balance with search engine operators dereferencing beyond the EU.⁷⁷ This latter observation suggests that the Union has not acted reasonably vis-à-vis the extraterritorial dimensions of its right to erasure. It is not apparent that the legislature would have sought to extend dereferencing extraterritorially to safeguard rights to privacy and data protection.⁷⁸ The Court decision, in not immediately mandating global de-listing, covertly suggests its non-extraterritorial application would be the default, most reasonable approach.

The Court closes its judgement by affirming that national data protection authorities (such as CNIL) or national judicial authorities do have the competence to order dereferencing from all versions of a search engine.⁷⁹ They may weigh up the protection of fundamental rights to data protection and privacy against the right to freedom of information, and may order the search engine operator to carry out global delisting.⁸⁰ The Court seems to hand over the task of conducting an interest- and rights-balancing test to national authorities. National data protection supervisory authorities are neither elected nor part of the court structure, which could avoid necessary checks, balances and harmonisation, but foreign entities with an EU connection (such as Google Inc. with an establishment in France) that are affected by a decision of a national regulatory authority may challenge it before a court. Individual internet users without an EU connection, however, may not, which could be problematic. These data protection authorities have the opportunity to make non-EU users see an 'EU' version of Google. It is unclear whether this will materialise or not, but given their pro-data protection stance and trend towards allowing or calling for extraterritoriality, it would not be surprising if the data protection authorities obliged global delisting from within their own jurisdictions. It flows from this that the authorities should follow the CJEU's example in the *Google v CNIL* case and exercise reasonableness in making such decisions. This reasonableness involves

⁷⁶ *ibid* 67.

⁷⁷ *ibid* para 61.

⁷⁸ *ibid* para 62.

⁷⁹ *ibid* para 72.

⁸⁰ *ibid*.

requiring strong connections between data subjects in the EU and search engine users outside the EU, and balancing the various interests and rights, which would ordinarily lead to maintaining EU-wide dereferencing as the default position.

On a similar note, the CJEU recently left the door open to the extraterritorial application of EU law and again deferred to national authorities to determine when this may be warranted.⁸¹ The *Eva Glawischnig-Piesczek v Facebook* case pertained to the potential global effects of the Electronic Commerce Directive.⁸² The Court considered whether content considered defamatory in an EU Member State should be blocked on social media platforms with worldwide effect. It ruled that the Directive does not preclude EU Member State courts from ‘ordering a host provider to remove information covered by the injunction or to block access to that information worldwide within the framework of the relevant international law’.⁸³ Once again, the Court has reasonably not required global blocking. It has also not excluded this possibility, giving that interest- and rights-balancing exercise to national courts to conduct on a case-by-case basis in line with international law. The Court simply said this was not contrary to EU law. The judgement is normatively different from that in *Google v CNIL*. For instance, it barely mentions fundamental rights and does not mention the divergent approaches to fundamental rights in different countries, as the Court did in the latter case. It is nonetheless important because its approach to EU law extraterritorially on the internet is conceptually similar to that in the *Google v CNIL*. It also remains to be seen how individual Member States will implement the decision.

4. Conclusion

Using reasonableness can reduce the importance or even need for territorial links to establish jurisdiction, which is important in the online

⁸¹ *Eva Glawischnig-Piesczek v Facebook Ireland Limited*.

⁸² *ibid*; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the internal market [2000] OJ 2000 L178.

⁸³ *ibid* 53.



sphere where most data processing occurs.⁸⁴ The EU must ensure its data subjects (ordinarily residents)' fundamental right to data protection is safeguarded. This is bearing in mind the other rights and considerations – particularly stemming from third State jurisdictions – against which the right to data protection ought to be balanced and instances where the right may be limited. Accordingly, beyond traditional permissive principles of jurisdiction and fundamental rights obligations, the EU should exercise extraterritorial jurisdiction in the data protection sphere with restraint to reduce conflicts between States seeking to regulate the same situation. The Third and Fourth Restatement of US Foreign Relations Law outline other considerations, such as the degree of connection between a State and a situation, that can inform the EU's jurisdictional claims. Within both Restatements, a spirit of reasonableness is important. Accordingly, the EU should use reasonableness that includes interest- and rights- balancing to mitigate any problematic jurisdictional overreach as a result of the application of its data protection laws.

⁸⁴ Buxbaum (n 15) 650 (citation omitted).

