BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 2 • N° 6 • MAY 2016

PERMISSIONS AND PROHIBITIONS IN DATA PROTECTION JURISDICTION

by Mistale Taylor[1]

Abstract

Under public international law, a State has a right to exercise jurisdiction and is expected to show restraint when applying extraterritorial jurisdiction. The EU's Data Protection Directive is far-reaching and has notable effects beyond its territory. The General Data Protection Regulation could serve to broaden these external effects. This expansive application of prescriptive jurisdiction has caused jurisdictional tensions between, for instance, the EU and the US. EU data protection law could conceivably fall into traditional public international law permissive principles of jurisdiction, such as subjective territoriality, objective territoriality, passive personality or the effects doctrine. Whilst there appears to be a shift from territory to personality in European data protection law, territory is still necessary to trigger the application of jurisdiction. The demarcations provided by public international law could offer ways to mitigate transatlantic conflicts in jurisdiction.

Keywords: jurisdiction – data protection – public international law – extraterritoriality

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html

ISSN N° 2565-9979. This version is for academic use only.

Disclaimer

1. Introduction

Oftentimes, and particularly in the EU-US privacy law interface, there exist situations in which more than one State could have the competence to exercise jurisdiction; multiple States might have legitimate claims to regulate the same situation. Indeed, overlapping jurisdictional claims could be seen as a reality of international law, amplified in the digitised data-sharing sphere due to globalisation and interconnectivity brought on by technology.[2] This reality, however, can and does easily lead to conflicting regulation and jurisdictional tensions between States, which can be problematic.[3] Transatlantic tensions over the apparent extension of EU data protection law into US territory have inspired legal clashes between the two jurisdictions. Even though such clashes exist between the EU and other third States, the present research focuses on the transatlantic divide because the value-based legal approaches to privacy are markedly different in the Union and the US. There have thus been many clashes that lend themselves to being explored with a public international law perspective.

Jurisdiction in public international law regulates a State's application of power through that State's laying down the law, hearing and investigating cases, and administering the law. These three categories are commonly respectively labelled prescriptive or legislative, adjudicative or judicial, and enforcement jurisdiction.[4] Jurisdiction is closely connected to cornerstone principles of public international law: state sovereignty and non-intervention. As such, the main principle permitting a State to exercise jurisdiction in a particular situation is territoriality, that is, a State may regulate conduct within its territorial boundaries. Whilst there exists in public international law a presumption against exercising jurisdiction beyond one's borders, that is, extraterritorially, there are several permissive principles that could allow the exercise of such jurisdiction depending on the circumstances.[5] These principles extend to where an act is initiated or consummated (subjective and objective territoriality); a person's nationality (personality or nationality); the protection of a State's vital interests (protective); the ramifications of an act felt within a State (effects doctrine); and crimes against all that could entail *jus cogens* or *jure gentium* norms and spark obligations *erga omnes* (universal). It is perhaps only the last category of universal jurisdiction that could in theory admit of the exercise of wholly extraterritorial jurisdiction without any territorial connection between a situation and its regulation.

There are numerous examples of the expansive application of EU law where the territorial nexus between the regulator and situation is weak. For instance, EU law could apply when personal data is transferred from an EU Member State to a US incorporated company, or when a US company collects browsing data of an EU resident on EU territory. The US has often contested this apparent expansive application of EU law, which has led to clashes. Such clashes have in turn resulted in, *inter alia*, legal uncertainty, forum shopping and misused resources, all of which could ultimately threaten the protection of EU citizens' fundamental right to protection of their personal data.[6]

---

1 Mistale Taylor LLM, PhD candidate at Utrecht University and Senior Research Associate at Public International Law and Policy Group. The author would like to thank Professor Cedric Ryngaert, Professor John Vervaele and Professor Christopher Kuner for comments on an earlier draft. The research that resulted in this publication was funded by the Dutch Organisation for Scientific Research under the VIDI Scheme.

2 Mills, Alex, 'Rethinking Jurisdiction in International Law', *British Yearbook of International Law*, Vol. 84, No. 1, pp. 187-239, 2013, p. 197.

3 *Idem* at pp. 199-200.

4 Restatement of the Law Third, The Foreign Relations Law of the United States §401; *Model Plan for the Classification of Documents Concerning State Practice in the Field of Public International Law*, Council of Europe Res (68) 17 of June 1968.

5 See, e.g., Crawford, James, *Brownlie's Principles of Public International Law*, OUP: Oxford, 2012, p. 486.

6 Indeed, European regulators have somewhat acknowledged this clash, albeit in reverse. The General Data Protection Regulation (GDPR) (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, OJ L 119, 04.05.2016) provides that "[t]he extraterritorial application of [third State legislation] may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union" (recital 115). This provision also emphasises the EU's continuing concern for its residents' right to data protection in extraterritorial situations.

Nonetheless, these tensions and the negotiations, renegotiations and attempts to find compromises, however arduous, might not be entirely negative. They have, for example, obliged parties to accommodate aspects of each other's value-based legal traditions in privacy law, which is a positive development in a pluralistic world. It is beneficial for EU residents and the States involved, however, to have these jurisdictional conflicts mitigated. Indeed, the very purpose of "jurisdiction", it being ultimately the regulation of a State applying sovereign power, could demarcate and thus restrict a State's authority to act, which could reduce inter-State conflicts.[7]

The present article starts from the premise that the EU has fundamental rights obligations in relation to its data protection laws with extraterritorial effect.[8] The Union could be understood to have a duty or obligation to exercise extraterritorial jurisdiction under international human rights law, as a subset of public international law. Public international law is used as an overarching system to demarcate the EU's exercise of jurisdiction. Whilst international human rights law casts a wide jurisdictional net, public international law jurisdiction aims to limit far-reaching jurisdictional claims.[9] This research reinterprets the existing principles of jurisdiction for the data protection legal sphere to illustrate how provisions in EU data protection instruments can fall within multiple permutations of multiple forms of jurisdiction.

Firstly, the research outlines classic approaches to jurisdiction under public international law. It then looks at applicable law provisions and important definitions in the current Data Protection Directive (DPD) and the General Data Protection Regulation (GDPR), which entered into force in May 2016 and will apply from May 2018.[10] The bulk of the research lays out ways to exercise territory- or personality-based jurisdiction over situations with an extraterritorial dimension. It attempts to see if and how the DPD and GDPR could fit into these principles. The research's underlying question is how the classic permissive principles of territorial and personality jurisdiction in public international law can be interpreted to accommodate EU data protection legislation, ultimately to delimit the EU's exercise of extraterritorial prescriptive jurisdiction. It purports to show how territory-based jurisdiction as in the DPD is moving closer to a form of personality-based jurisdiction in the GDPR.

2. Public International Law Approaches to Jurisdiction

Below is an outline of how the present article understands jurisdiction under public international law. It focuses on prescriptive jurisdiction in the data protection sphere as opposed to adjudicative or enforcement jurisdiction. Whilst there are examples of the EU exercising the latter two extraterritorially, the EU has arguably had most influence in prescribing the law abroad, either directly or indirectly, so we can draw stronger conclusions from these actions.[11]

Although its actions may be addressed towards an actor including another State; a non-State actor such as a corporation; or, increasingly, an individual, the State is the exclusive agent in exercising jurisdiction under public international law. The present research equates EU action with State action. This is not only because Member States have handed over many competences to the EU, but also because they have implemented the DPD, albeit not uniformly, into national law. The GDPR's

7 Ryngaert, Cedric, *Jurisdiction in International Law* (2nd ed.), OUP: Oxford, 2015, p. 29: jurisdiction has a regulating purpose in "delimiting States' spheres of action and thus reducing conflicts between States".

8 Taylor, Mistale, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect', *International Data Privacy Law*, Vol. 5(4), 2015, pp. 246-256, pp. 255-256.

9 Ryngaert (n 6), p. 23.

10 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 (DPD); GDPR.

11 Examples of the EU exercising indirect prescriptive jurisdiction extraterritorially include the influence of the DPD's adequacy requirement (Article 25) on third State law. EU Courts can also exercise prescriptive jurisdiction by, for example, interpreting EU legislation according to international law principles – see Ryngaert (n 6), p. 10.

provisions will be directly applicable in Member States. As such, Member State law reflects EU law and *vice versa*. Furthermore, the EU is bound by the customary international law of jurisdiction.[12]

2.1. The Supposed Illegitimacy of Extraterritorial Jurisdiction

The well-known Permanent Court of Arbitration *Island of Palmas* judgement (1928) established that when settling most questions of inter-State relations, we begin with the notion that a State has exclusive competence regarding its own territory.[13] Exercising jurisdiction becomes an issue and consequently a question of international law when a State attempts to regulate matters that go beyond its own territory and exclusively domestic concerns.[14] In the also renowned *Barcelona Traction* judgement (1970), it was acknowledged that State sovereignty and non-interference principles require limits imposed by international law on the exercise of jurisdiction in cases with foreign elements.[15] With a view to preserving State sovereignty, there has traditionally existed a presumption against exercising extraterritorial jurisdiction. That said, even in the 1927 Permanent Court of International Justice *Lotus* judgement (discussed *infra*), the judges anticipated the diminishing relevance of physical borders.[16] In addition, in their joint individual opinion in the 2000 *Arrest Warrant* case, three judges noted a move "towards bases of jurisdiction other than territoriality".[17] Such a presumption against extraterritoriality is becoming increasingly obsolete, or less controvertible, due in part to legal questions raised in the online sphere.[18]

2.2. Two Approaches to Lawfulness under Public Internationa Law

There are two main approaches when exercising jurisdiction, with the first enshrined in a prominent case and the second being most commonly applied in practice.[19] Firstly, a State could be allowed to exercise jurisdiction as desired, unless such abandon were limited by a prohibitive rule to the contrary. This approach was established in landmark jurisdiction case, the *Lotus* case.[20] That case involved a collision between a Turkish steamer (S. S. *Boz-Kourt*) and a French steamer (S. S. *Lotus*) on the high seas, which resulted in the death of eight Turkish citizens.[21] Upon the S. S. *Lotus*' arrival in Turkey, Turkish officials initiated criminal proceedings against the French officer of the watch who had been on board the steamer during the collision.[22] France eventually brought a case before the Permanent Court of International Justice to determine whether Turkey's exercise of criminal

12 CJEU, *Air Transport Association of America and Others v Secretary of State for Energy and Climate Change*, Case C-366/10, 21 December 2011, paras 101 and 123: "[the EU] is bound to observe international law in its entirety, including customary international law, which is binding upon the institutions of the European Union".

13 Island of Palmas Case (or Miangas), *United States v Netherlands,* Award, (1928) II RIAA 829, ICGJ 392 (PCA 1928), 4th April 1928, at 838; see too 'Draft Convention on Jurisdiction with Respect to Crime', *The American Journal of International Law*, Vol. 29, Supplement: Research in International Law (1935), pp. 439-442, Art. 3.

14 Ryngaert (n 6), p. 5 *cit*. Mann, Frederick A. 'The Doctrine of Jurisdiction in International Law', Recueil des Cours 111, 1964, pp. 1–1621, p. 9.

15 Case concerning Barcelona Traction, Light and Power Co Ltd (*Belgium v Spain*), Separate Opinion of Judge Sir Gerald Fitzmaurice, (1970) ICJ Reports 65, para. 70.

16 *S.S. "Lotus", France v Turkey*, PCIJ, Series A, No. 10. 1927; 4 AD, para 45, which states that "[t]he territoriality of criminal law, therefore, is not an absolute principle of international law and by no means coincides with territorial sovereignty"; Ryngaert (n 6), p. 33 *cit.* Mann (n 13), p. 36.

17 As Judges Higgins, Kooijmans and Buergenthal pointed out in their joint individual opinion in the *Case Concerning the Arrest Warrant of 11 April 2000* (*Democratic Republic of the Congo v Belgium*) [2002] ICJ 1, para 47.

18 Acting extraterritorially is unsurprisingly linked to preserving national interests and it has been asserted that public international rules hardly restrain State action in practice. See, e.g., "States increasingly perceive the need to protect both their own interests and the interests of the international community in respect of conduct occurring beyond their borders" - Kamminga, Menno T., 'Transnational Human Rights Litigation against Multinational Corporations Post-*Kiobel*', in: *What's Wrong with International Law?: Liber Amicorum A.H.A. Soons*, Cedric Ryngaert, Erik J. Molenaar and Sarah Nouwen (eds.), Brill Nijhoff: Leiden, 2015, pp. 154-165, p. 157; "courts often only pay lip-service to the territoriality presumption" – Ryngaert (n 6), p. 77 (citations omitted).

19 Ryngaert (n 6), p. 23.

20 *S.S. "Lotus"* (n 15), paras 45-49.

21 *Idem* at para 2.

22 *Ibidem*.

jurisdiction over a foreign national for an incident that happened outside Turkey's territorial jurisdiction was a violation of international law. The Court decided that Turkey's exercise of jurisdiction, lacking a prohibitive rule to the contrary, was lawful.[23] The *Lotus* decision, however, has since been criticised, in part because it confers a burden upon States to prove a rule prohibiting the exercise of jurisdiction exists, which does not match current State practice.[24]

The second main approach prohibits States from exercising jurisdiction unless there is a positive rule permitting them to do so. Customary international law, most States and most doctrine support this approach.[25] As such, States are expected to act with restraint when exercising jurisdiction. They have a right to exercise jurisdiction at their own discretion, but do not necessarily have to regulate to the full extent that international law permits.[26] The State has an option, not necessarily an obligation, to exercise power. This discretion, however, could be evolving into a duty, especially in international human rights law.[27] In specific situations with a foreign element, States may exercise jurisdiction, as explored below.

2.3. A Substantial Connection

A regulating State should have a genuine connection with the situation over which it claims prescriptive jurisdiction.[28] Public international law allows for a State with a strong, ordinarily territorial connection to a situation to regulate that situation.[29] Another understanding of "connection" under public international law posits that a State can exercise extraterritorial jurisdiction if it does not interfere with another, more closely connected State's right to do so.[30] Similarly, under conflict of laws or private international law, the State exercising jurisdiction must have the strongest connection to a situation over which multiple States could claim jurisdiction.[31] The "greater connection" threshold has been conflated with both public and private international law.[32] It is thus difficult to establish precisely what constitutes a substantial and direct connection to a situation to permit a State's exercise of jurisdiction, and whether this connection need only be strong or rather the strongest.

23 *Idem* at paras 45-49.

24 See for example, Shaw, Malcolm, *International Law,* 7th ed., Cambridge University Press: Cambridge, 2014, p. 477.

25 See, e.g. *Arrest Warrant* (n 16) (Joint separate opinion of Judges Higgins, Kooijmans and Buergenthal), paras 49-50 and Dissenting opinion of Judge ad hoc Van den Wyngaert, para 51; Crawford (n 4), p. 477.

26 Mills (n 1), pp. 187-239, p. 199 *cit.* Mann (n 13) p. 3 - "Jurisdiction involves a State's *right* to exercise certain of its powers" (emphasis in original); this sentiment is echoed in *Arrest Warrant*: "a State is not required to legislate up to the full scope of the jurisdiction allowed by international law" – *Arrest Warrant* (n 16) (Joint separate opinion of Judges Higgins, Kooijmans and Buergenthal), para 45.

27 See, e.g., Mills (n 1), pp. 187-239, p. 187; Ryngaert (n 6), p. 22.

28 See, e.g., Kuner, Christopher, 'Jurisdiction on the Internet: Part II', *International Journal of Law and Information Technology*, Vol. 18(3), 2010, pp. 227-247, p. 237 *cit., inter alia,* International Law Commission (ILC), 'Report on the Work of its Fifty-Eighth Session' (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10, Annex E, para 42.

29 Ryngaert (n 6), p. 19; Svantesson goes so far as to suggest substantial connection replace territory as a permissive principle to exercise jurisdiction in both public and private international law – Svantesson, Dan Jerker B., "A New Jurisprudential Framework for Jurisdiction", *AJIL Unbound*, Vol. 109, pp. 69-74, p. 74.

30 Currie, John H., *Public International Law*, Irwin Law: Toronto, 2001, p. 299.

31 Ryngaert (n 6) p. 19.

32 Mills, who has written extensively on the differences and similarities between public and private international law, posits that "the exercise of international jurisdiction by each state aspires to avoid a conflict through openness to the application of foreign rules which have a greater 'connection' to the dispute at hand, as determined and shaped by public and private international law rules and principles" – Mills (n 1), p. 209.

The general public international law principles discussed below cover some of the links or connections needed to establish a State's basis for exercising jurisdiction.[33] That statement appears more straightforward and simplistic than its application in practice, however. The permissive principles are not clear cut; especially in the data protection examples they often overlap; they are not without contestation; and in general "must be employed with great caution".[34]

2.4. Permissive Principles

Permissive principles of jurisdiction in public international law concern links between a situation and a State's related authority to prescribe, adjudicate or enforce the law governing that situation. These principles consist of, *inter alia,* territoriality (including the effects doctrine) and personality, upon which the present focuses. Other principles not discussed here include protectivity and universality. The State to situation link is not always hinged upon territory. When a State claims jurisdiction under one of the extraterritorial principles, it often inspires controversy and protest by other States. This remonstration does not necessarily render such claims unlawful or illegitimate. By the same token, if a State's claim to jurisdiction falls within one of the below principles, that does not *per se* connote lawfulness or legitimacy.[35] According to the Third Restatement of US Foreign Relations Law, an authority on extraterritorial jurisdiction, a State claiming extraterritorial prescriptive jurisdiction must foremost adhere to one of the principles to be permitted to do so.[36] Thereafter, threshold requirements apply and include the State's degree of link/connection to the situation, its interests and how reasonable its exercise of jurisdiction is.[37]

This research accordingly proceeds from the understanding that: (i) the EU's data protection law has extraterritorial effects; (ii) States may not exercise jurisdiction unless expressly permitted to do so; (iii) there should exist a substantial link between the regulating State and a situation; and (iv) classic public international law jurisdictional principles can demarcate how and when the EU may exercise (extraterritorial) jurisdiction. Multiple States may lay claim to applying the abovementioned forms of jurisdiction to the same situation.

Regulation in EU data protection law overlaps when a third State data controller or processor is required to comply with EU data protection law (Article 4 DPD; Article 3 GDPR) or when the DPD or GDPR require a State to enact laws in line with those in the EU to receive data transfers from the EU (Article 25 DPD; Article 45 GDPR). International tensions arise when US and EU laws could apply to a situation and US laws run counter to EU data protection principles. The following introduces the relevant parts of EU data protection law, which are then woven into an analysis of the major permissive principles of extraterritorial jurisdiction to discern under which principles the DPD and GDPR could fall.

33 This sentiment is confirmed by, for instance, the International Law Commission's statement that "[t]he types of connections that may constitute a sufficient basis for the exercise of extraterritorial jurisdiction are reflected in the general principles of international law which govern the exercise of such jurisdiction by a State" – Kuner (n 27) p. 237 *cit., inter alia,* International Law Commission (ILC), 'Report on the Work of its Fifty-Eighth Session' (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10, Annex E, para 42; see, too, "[w]hat is a 'sufficient connection' may be established initially with reference to certain general principles of jurisdiction**"** - Kamminga, Menno, 'Extraterritoriality', in Wolfrum, R. (ed.), *Max Planck Encyclopaedia of Public International Law*, OUP: Oxford, 2011, §10.

34 Kamminga (n 32) §10.

35 Svantesson, Dan Jerker B., *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing: Denmark, 2013, p. 84.

36 US Third Restatement (n 3) *§§* 402-403.

37 *Ibidem*; it has been suggested the classic principles are substitutes for the second-tier requirements (Ryngaert, Cedric, 'An Urgent Suggestion to Pour Old Wine into New Bottles – Comment on "A New Jurisprudential Framework for Jurisdiction", *AJIL Unbound*, Vol. 109, pp. 81-85, p. 82). If the second-order criteria are so analogous to the first, then it makes sense to analyse them.

3. EU Data Protection Basics

This section outlines the provisions in the DPD and GDPR that inform the subsequent analysis. The DPD is the only data protection instrument of its kind to clarify its jurisdictional scope, making it the ideal text to analyse when attempting to find some jurisdictional limits to EU data protection law.[38] Earlier proposals for the DPD and its preamble show that the drafters aimed to delineate applicable law to avoid data processors relocating to escape the reach of the Directive.[39] This had the ultimate aim of protecting EU data subjects. If data processors could avoid having the Directive cover their activities simply by moving out of EU territory, this would mean the Directive's scope was entirely territorial. The fact that the drafters aimed to prevent this possibility to forum shop means they might have, purposefully or inadvertently, broadened the DPD's scope of application so much as to have extraterritorial effect. In revising the DPD, the European Commission had the comparable aim to "revise and clarify the existing provisions on applicable law [ultimately to] provide for the same degree of protection of EU data subjects, regardless of the geographic location of the data controller".[40]

3.1. Applicable Law and Jurisdiction

Based on the wording in the DPD, this research equates prescriptive jurisdiction with which law applies – to a certain extent. That is, if the DPD as implemented by a Member State applies to a certain situation, the EU can be understood as ultimately exercising prescriptive jurisdiction by having laid down the law that should apply to that situation. In scholarly analyses of the differences and similarities between applicable law (as Article 4 DPD "national law applicable" appears to be) and jurisdictional scope, a generally-accepted conclusion is that prescriptive, but not necessarily adjudicative or enforcement, jurisdiction in the data protection context are comparable.[41] Moreover, the two often overlap in extraterritorial situations.[42] This research thus equates applicable law in the DPD to prescriptive jurisdiction. Indeed, it is highly likely that a State would seek to apply its own law and not foreign law to a situation. Private international law can readily solve some jurisdictional clashes, however it draws more parallels with adjudicative rather than prescriptive jurisdiction.[43]

3.2. Data Controllers and Data Processors

Distinguishing between data controllers and data processors is important when looking at the ex-

38 Kuner, Christopher, 'Jurisdiction on the Internet: Part I', *International Journal of Law and Information Technology*, Vol 18(2), 2010, pp. 176-193, p. 186 and Svantesson (n 34) p. 89 *cit.* Bygrave, Lee, 'Determining applicable law pursuant to European Data Protection Legislation', *Computer Law and Security Report* Vol. 16, 2000, pp. 252-257, p. 252.

39 Svantesson (n 34), see p. 96, fn 203 *cit.* COM (92) 422 final, SYN 287, 15 October 1992, p. 13: to avoid the possibilities "that the data subject might find himself outside any system of protection, and particularly that the law might be circumvented in order to achieve this; [or] that the same processing operation might be governed by the laws of more than one country" and p. 95 *cit.* Kuner, Christopher, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed., OUP: Oxford, 2007, p. 111: "[t]he intent of the drafters was [*inter alia*] to prevent the possibility of evading EU rules through the relocation of data processing to third countries"; see also recital 20 in DPD preamble: "[w]hereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive".

40 European Commission, 'A comprehensive approach on personal data protection in the European Union', COM (2010) 609 final of 4.11.2010, p. 11.

41 Colonna, Liane, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?', *International Data Privacy Law*, Vol. 4(3), 2014, pp. 203-221, p. 208: "[e]ven though applicable law and jurisdiction are two legally distinct concepts, in practice, applicable law provisions may also govern questions of jurisdiction, at least in the context of data protection". *cit.*, *inter alia*, Kuner, Christopher, *Transborder Data Flows and Data Privacy Law*, OUP: Oxford, 2013. See the *Weltimmo* judgement, however, which separates jurisdiction from applicable law. The CJEU ruled that national data protection supervisory authorities may investigate complaints (thus exercising adjudicatory or enforcement jurisdiction) regardless of the national law applicable. This is in an intra-EU context, however, and is not necessarily applicable to prescriptive jurisdiction with external effects, which we examine here. CJEU (Third Chamber), Reference for a preliminary ruling in Case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 October 2015, para. 57.

42 Kuner, Christopher, 'Extraterritoriality and regulation of international data transfers in EU data protection law', *International Data Privacy Law*, Vol. 5(4), 2015, pp. 235-245, p. 236.

43 Ryngaert, Cedric, 'The Concept of Jurisdiction in International Law' in Orakhelashvili, Alexander (ed.), *Research Handbook on Jurisdiction and Immunities in International Law*, Edward Elgar Publishing Limited: Cheltenham, 2015, pp. 50-75, p. 59.

traterritoriality of EU data protection law in part because the applicability of many of the DPD's provisions hinges upon the characterisation of an entity as controller or processor, and its location. Whether an entity is a controller or processor can be ambiguous and difficult to determine, and multiple entities can be considered controllers.[44] In essence, however, a processor is supposed to process personal data according to the controller's direction.[45] This can consequently inform the jurisdictional reach of the DPD.

The DPD defines a controller as follows:
[T]he natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data […];[46]
A data controller is thus responsible for the personal data. Examples of controllers include corporate bodies and Non-Governmental Organisations. An individual, such as a doctor keeping personal information about patients or a self-employed consultant keeping personal information about clients, could also be a data controller.[47]

A data processor is outlined in the DPD as the following:
[A] natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller; [48]
Accountants, market research companies and internet service providers would normally be considered data processors. The controller and processor are discrete legal entities.[49] For instance, a food delivery company that outsources its ordering service to a call centre would be considered the data controller (responsible for its customers' personal data, such as name, address, and phone number) and the call centre would be the data processor (processing this personal data on the company's behalf). The GDPR defines controllers and processors in the same way as the DPD.[50] Notably, however, the GDPR confers some accountability obligations on the processor as well as the controller.[51] Following the above outline of the relevant EU data protection terms, the next section looks at other provisions in the DPD and GDPR, and fits them into the main basis for exercising jurisdiction: territoriality.

4. Territoriality

As it has different meanings depending on the field of law, this section will look at territorial jurisdiction in terms of data protection law on the internet in an EU context.[52] The internet has become the leading example of a "space" or "place" that is difficult to link directly with a physical territory. It thus raises challenges for traditional claims of jurisdiction premised on territorial sovereignty. The internet is popularly referred to as representing "deterritorialization, transnationalism, state decline, and the replacement of national pyramids of normativity by global networks of spread-out normativity".[53] This characterisation calls into question using territoriality as an analytical lens.

44 Kuner, Christopher, *European Data Protection Law: Corporate Compliance and Regulation*, 2nd ed., OUP: Oxford, 2007, pp. 69-73.
45 *Idem* at p. 70.
46 DPD, Art. 2(d); GDPR, Art. 4(7) reads almost entirely the same.
47 For practical examples, see Irish Data Protection Commissioner, 'Are you a "data controller"?', *available at* https://www.dataprotection.ie/docs/Are-you-a-Data-Controller/y/43.htm.
48 DPD, Art. 2(e); GDPR, Art. 4(6) reads almost entirely the same.
49 Article 29 Working Party, 00264/10/EN WP 169 Opinion 1/2010 on the concepts of "controller" and "processor", 16 February 2010, p. 1.
50 GDPR, Arts. 4(7) and 4(8). The DPD refers to "national or Community law" where the GDPR uses "Union or Member State law", which is a negligible difference for our purposes.
51 Ustaran, Eduardo, 'EU General Data Protection Regulation: things you should know', *Privacy and Data Protection*, Vol. 16(3), 2016, p. 4. For instance, the GDPR (Arts. 3(1) and 3(2)) applies to data processing by controllers or processors where the DPD (Art. 4) applies only to controllers.
52 Ryngaert (n 6) p. 218, fn 138 *cit.*, e.g., Note, 'Predictability and Comity: Toward Common Principles of Extraterritorial Jurisdiction', *Harvard Law Review*, Vol. 98(6), 1985, p. 1310.
53 Schultz, Thomas, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/PublicInternational Law Interface', *European Journal of International Law*, Vol. 19, No. 4, 2008, p. 801 *cit.* Goldsmith, Jack and Wu, Tim, *Who Controls the Internet? Illusions of a Borderless World*, OUP: Oxford, 2006, p. 179, pp. 181 – 183.

As exciting as the prospect sounds, however, the internet is not necessarily so borderless and global. [54] One could rephrase that in terms of jurisdiction: exercising jurisdiction in the virtual data protection sphere is not usually divorced from territory. Indeed, a territorial nexus to a situation is required to trigger the application of the DPD. Often this nexus is somewhat far-fetched and could admit of the Directive's broad application, which is partly what has inspired the conflicts between the perhaps aggressive reach of EU law and the US' own exercise of jurisdiction.

Whereas the DPD refers repeatedly to "territory" in the article entitled "national law applicable",[55] the GDPR instead uses "in the Union", which could suggest an area not necessarily physical.[56] The GDPR article, however, is called "territorial scope", potentially bringing physical territory back into the picture.[57] In his opinion in the *Salemink* case, the Advocate General asserted that "for EU purposes, the 'territory' of the Member States is the area (not necessarily territorial, in the spatial or geographical sense) of exercise of the competences of the Union", calling the connection between exercising sovereignty and a physical territory closer to a contingent, rather than a necessary, truth.[58] To be able to continue a discussion on territorial and extraterritorial jurisdiction, however, we employ the term "territory" here to mean the physical or geographical space of a State or the EU. This justifies discussing extraterritoriality in the traditional public international law sense; if we used "territory" to cover all areas in which Member States and EU institutions implemented EU law, there would arguably be no extraterritorial application of the law. Nonetheless, redefining territory in the cybersphere could help clarify how EU data protection law applies, as physical boundaries are indeed becoming less relevant and EU territory as non-physical space is a compelling idea.

The territoriality principle is certainly important in questions of the EU's exercise of jurisdiction in the cybersphere. In 2003, for instance, the CJEU affirmed in the landmark *Lindqvist* decision that EU law does not apply indiscriminately to the whole internet.[59] In that case, Mrs. Lindqvist had uploaded personal data, such as names and phone numbers, of her fellow parish volunteers onto her own webpage.[60] She was charged with violating Swedish data protection law because she had processed personal data by automatic means without first notifying the Swedish data protection supervisory authority; she had processed sensitive data without authorisation; and she had transferred data to third States without authorisation.[61] The CJEU made several landmark pronouncements on EU data protection law in *Lindqvist*, but the most relevant one for our purposes relates to the third issue of data transfers to third States.[62] The Court held that simply being in the EU and uploading personal data to a web page, which anyone in the world with internet access could access, did not constitute the transfer of personal data to a third State.[63] This ruling was important because the DPD only allows personal data to be transferred outside the EU if that third State offers adequate data protection. As such, the Court limited the scope of application of EU law: not every State with internet users who accessed EU pages needed an official acknowledgement of adequate data protection.

54 Schultz (n 52) p. 801.
55 DPD, Art. 4: "established on the Member State's territory […] established on Community territory […] situated on the territory".
56 GDPR, Art. 3.
57 *Ibidem*.
58 AG Opinion, *Salemink*, Case C-347/10, 8 Sept., 2011, paras 54-57; see also Bartels, Lorand, 'The EU's Human Rights Obligations in Relation to Policies with Extraterritorial Effects', *The European Journal of International Law*, Vol. 25(4), 2015, pp. 1071-1091, p. 1088, which also cites the *Salemink* AG Opinion.
59 CJEU, Judgement of the Court of 6 November 2003 in Case C-101/01 (Reference for a preliminary ruling from the Göta hovrätt): *Bodil Lindqvist*, OJ 2004 C7/3, §71: there is no data transfer that falls within the scope of Art. 25 DPD on data transfers to third States first requiring adequacy decisions, "where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country".
60 *Idem* at §2.
61 *Idem* at §15.
62 *Idem* at §23.
63 *Idem* at §71.

In revising data protection instruments, there appears to be a move from "territory" to "jurisdiction", perhaps somewhat de-emphasising the link between territory and a State's authority to regulate. The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) provides the most pertinent example, which can colour the discussion on territory in the DPD.[64] Since 2011, various data protection experts have been working on updating the 1981 Convention.[65] The amendments to the Convention are far from being finalised. During the still-ongoing discussion and consultation phase, there have been three notable developments regarding jurisdiction. Firstly, the 2012 modernisation proposal changed the text of the Convention's object and purpose article from reading that the Convention's purpose is to secure respect for rights and freedoms "*in the territory* of each Party for every individual, whatever his nationality or residence" to securing them "for every individual *subject to the jurisdiction* of the Parties, whatever their nationality or residence".[66] Aside from it bringing Convention 108 into line with the European Convention on Human Right's jurisdictional scope and allowing for international organisations to ratify the Convention more easily, this change was recommended because "referring to the concept of jurisdiction, rather than territory, [would seem most likely] to stand the test of time and continual technological developments [and] would seem more amenable to legal interpretation and more adaptable".[67] This recommendation seems to confirm that having jurisdiction over something that is not necessarily physical – rather like "the Union" *supra* – might be more suitable in the data protection field. Interestingly, the 2015 proposal has done away with territory and jurisdiction all together in the object and purpose article, suggesting it read that the Convention's purpose is "to protect every individual, whatever his or her nationality or residence".[68] This appears to sideline jurisdictional principles based on both territory and nationality or place of residence, although the aforementioned versions also make the effort to avoid discrimination based on nationality or place of residence.

Secondly, the scope article of the same Convention shows a move towards jurisdiction and a focus on the data subject, which is notable for the below discussion on the growth of personality-based jurisdiction in data protection. The Convention went from applying "to automated personal data files and automatic processing of personal data"[69] to "data processing subject to [the Convention's] jurisdiction [...] thereby securing every individual's right to protection of his or her personal data".[70] Here, the proposal drafters have added jurisdiction to the scope article, attaching it to both a data processing act and an individual.

Finally, the suggested changes to the article covering transborder flows of personal data reflect a move from territory to jurisdiction. The 1981 version covers "transborder flows of personal data going to the territory of another Party",[71] whereas both the 2012 and 2015 proposals refer to data transfers to a recipient who is "subject to the jurisdiction of another Party".[72] This is in line with the 2001 Additional Protocol to Convention 108 on supervisory authorities and transborder data flows,

64 CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg (Convention 108), 1981.

65 CoE, 'Council of Europe response to privacy challenges - Modernisation of Convention 108'. This position paper was distributed at 32nd International Conference of Data Protection and Privacy Commissioners, 27-29 October 2010, Jerusalem, Israel; Convention 108 (n 63); See also González Fuster, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer: Cham, 2014, pp. 90-92.

66 Convention 108 (n 63), Art. 1 (emphasis added); Strasbourg, 18 December 2012 T-PD_2012_04_rev4_E (emphasis added), p. 2.

67 Memorandum on introducing the concept of jurisdiction into Article 1 of Convention 108 (5 September 2012, update) Jean-Philippe Moiny, Research Fellow, F.R.S.-FNRS (Belgian Scientific Research Foundation – CRIDS (IT Law Research Centre), University of Namur), p. 6.

68 Ad hoc Committee on Data Protection (CAHDATA) Draft Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)1, 05/03/2015), p. 2.

69 Convention 108 (n 63), Art. 3(1).

70 Ad hoc Committee on Data Protection (n 67) p. 3; the 2012 proposal reads almost identically: the Convention applies to "data processing subject to its jurisdiction, thereby protecting the right to protection of personal data of any person subject to its jurisdiction" - T-PD_2012_04_rev4_E (n 65) p. 3.

71 Convention 108 (n 63), Art. 12(2).

72 T-PD_2012_04_rev4_E (n 65) p. 6; Ad hoc Committee on Data Protection (n 67) p. 6.

which covers data transfers to a recipient that is "subject to the jurisdiction of a State or organisation that is not Party to the Convention".[73] Whilst the aforementioned articles do not nearly make territory irrelevant when determining how and when the Convention applies to a certain situation, they could represent a change, necessitated by technology developments and a need for malleability, in the approach to territory *vis-à-vis* jurisdiction. It will be interesting to see the effect these developments have in the EU, all Member States of which have ratified Convention 108.

In sum, whilst some commentators might suggest otherwise, territory is relevant and important when looking at jurisdiction and EU data protection law. Trends towards "territory" not being physical or "jurisdiction" replacing "territory" could have several ramifications. For instance, the terms could be interpreted flexibly to accommodate advancing technologies that do away with physical territory, such as cloud computing. On the contrary, understanding "territory" as something non-physical could pave the way for the EU to expand its jurisdictional reach through creative interpretation or by relying upon other, more controversial forms of triggering jurisdiction. The next section looks at the applicable law provisions in the DPD and GDPR in terms of territory.

4.1. In EU Data Protection Law

Jurisdiction in EU data protection law is enshrined in the Directive as below:

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

(a) the *processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State* […];

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

(c) the *controller is not established on Community territory* and, for purposes of processing personal data *makes use of equipment*, automated or otherwise, *situated on the territory* of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community […].[74]

Where a controller is established and where "equipment" is located are important as ways to trigger the application of the DPD. As it can apply to controllers established in third States, the Directive can have effects beyond EU territory. The Article 29 Working Party, which consists of Member State Data Protection Authority representatives, the European Data Protection Supervisor and European Commission representatives, offers recommendations and opinions on EU data protection law. The Article 29 Working Party suggests that "neither the nationality or place of habitual

73 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows, CETS No.181, Strasbourg, 8.XI.2001, Art. 2(1); this also raises the complex question of how to exercise jurisdiction in respect of organisations as non-State actors.

74 DPD, Art. 4 (emphasis added); whilst online data is always stored or processed on a computer in a specific physical location, it is increasingly difficult to determine this location. "Any personal data processed on the Internet will still have to be stored on a computer in a physical location. However, in light of increased data processing on the Internet, it is usually quite difficult to determine the place of storage or processing. Indeed, under scenarios such as cloud computing, the processing may take place in a number of States simultaneously. Thus, the question is whether, in the era of cloud computing, it makes sense to speak of the data being 'located' in a specific place." – Kuner (n 27) p. 238 (citations omitted).

residence of data subjects, nor the physical location of the personal data, are decisive" when determining applicable law.[75] If personal data is processed in whole or in part outside the EU and there exists a relevant (territorial) link with the EU through the establishment of a controller and the nature of its activities, or through the location of equipment, the DPD can apply.

The GDPR's jurisdiction Article is as follows:
Territorial Scope

1. This Regulation applies to the *processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union*, regardless of whether the processing takes place in the Union or not.

2. This Regulation applies to the processing of personal data of *data subjects who are in the Union* by a *controller or processor not established in the Union*, where the processing activities are related to:

(a) *the offering of goods or services*, irrespective of whether a payment of the data subject is required, to such data subjects *in the Union*; or
(b) the *monitoring of their behaviour* as far as their behaviour *takes place within the Union*.

3. This Regulation applies to the processing of personal data by a *controller not established in the Union*, but in a place where Member State law applies by virtue of *public international law*.[76]

Despite being called "territorial scope", the GDPR's application article moves away from being anchored explicitly in physical territory. The DPD has a wide scope of application and the GDPR has potentially an even wider one. Instead of simply the place of establishment of a controller criterion, it adds the place of establishment of a processor as a possible jurisdictional hook. It also explicitly states that the data processing does not necessarily have to take place in the EU for the GDPR to apply. Moreover, it replaces the complicated location of equipment criterion in the DPD with the offering of goods or services, or monitoring of behaviour of EU data subjects when they are in the Union or their behaviour takes place in the Union.

The DPD and GDPR confirm that territory is the main base upon which the EU may exercise jurisdiction. The GDPR confirms the abovementioned tendency to move away from the term "territory" to terms that could be construed more vaguely ("in the Union"). The next section looks at some of the main permissive principles of jurisdiction not hinged solely upon a territorial connection to a single State, and endeavours to fit EU data protection law into each category.

4.2. Subjective Territoriality

Subjective territoriality covers situations in which an act begins in one territory, but is completed in a different territory. Under this principle, the State in which the act was initiated could claim jurisdiction over the act. The EU law country of origin principle provides that where there is a conflict of laws when an act is performed in one State, but received in another, the law of the original State applies.[77] This draws parallels with the subjective territoriality principle, albeit within an intra-EU context. The scope articles of the DPD and, indeed, the GDPR lend themselves much more easily to the objective territoriality principle, especially in terms of prescriptive jurisdiction.

75 Article 29 Working Party, 0836-02/10/EN WP 179, Opinion 8/2010 on applicable law adopted on 16 December, 2010 *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp179_en.pdf, p. 8.

76 GDPR, Art. 3.

77 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 ('Directive on electronic commerce'), OJ L 178, 17.07.2000 P. 0001 – 0016, recital 22.

The DPD's adequacy requirement, which also appears in the GDPR, could be understood as an manifestation of the subjective territoriality principle.[78] The adequacy requirement provides that any transfer of personal data outside the EU is, with some exceptions, *per se* unlawful unless the European Commission has deemed that the third State adequately protects that personal data.[79] Over 100 States have data protection laws, many of which afford an EU level of data protection to personal data transferred to those States.[80] Indeed, many States have almost directly copied the DPD and incorporated it into their own legal system, showing some sort of legal diffusion, or, at a stretch, perhaps (inadvertent) exercise of prescriptive jurisdiction by the EU.[81] In lieu of an adequacy decision by the European Commission, data can be transferred based upon bilateral agreements, such as the now invalid EU-US Safe Harbour agreement or proposed Privacy Shield, model contractual clauses and binding corporate rules. In this example, EU law essentially applies not only where an act, namely, a data transfer, begins in the EU, but where the transfer terminates in a third State.[82] As such, it exemplifies something close to the subjective territoriality principle in that the potential interference would occur in the third State, yet EU law would pre-emptively apply. The EU could be understood as exercising a soft form of extraterritorial prescriptive jurisdiction.

4.3. Objective Territoriality

Objective territoriality imbues the State where an act is consummated with jurisdictional authority. Provisions in the DPD and, to an arguably greater extent, the GDPR, can be seen as examples of this principle. Here, we examine Articles 4(1)a and 4(1)c of the DPD.

4.3(a) In the Data Protection Directive

According to Article 4(1)a DPD, if a data controller has its main establishment not on EU Member State territory, but it processes data in the context of the activities of an establishment of the main controller on the territory of a Member State, EU data protection law could apply to this processing. As such, EU jurisdiction could be established by a data processing act occurring ultimately on EU soil. An establishment must carry out the "effective and real exercise of activity" in the relevant data processing context to qualify as such.[83] It follows that a server or computer almost certainly would not qualify as an establishment.[84] The main factor to consider when analysing whether a data processing act occurs in the "context of the activities" is the extent to which an establishment is involved in the activities in the data processing context.[85] The nature of the activities is of secondary importance.[86]

This form of jurisdiction can be illustrated by the landmark CJEU *Google Spain* case (2014).[87] In that case, a Spanish national sought to be able to request that Google Spain or Google Inc. remove apparently irrelevant search results about his past financial situation.[88] The Court considered questions of (i) the scope of application *ratione materiae* of the DPD; (ii) the territorial scope of the DPD; (iii) the responsibility of a search engine operator for the results it produces; and (iv) whether

78 DPD, Art. 25; GDPR, Art. 45.
79 DPD, Art. 25(4).
80 Greenleaf, Graham, 'Scheherazade and the 101 data privacy laws: Origins, significance and global trajectories', *Journal of Law, Information & Science, Special Edition: Privacy in the Social Networking World*, Vol. 23, No. 1, 2014; Greenleaf, Graham, 'The influence of European data privacy standards outside Europe: Implications for globalisation of Convention 108?', University of Edinburgh School of Law Research Paper Series No 2012/12, 2012, abstract.
81 *Idem* at pp. 10-13; interview with Christopher Kuner, 18th March, 2016.
82 Kuner (n 27) 240.
83 DPD, recital 19.
84 Art. 29 WP 2010 (n 74), p. 12.
85 *Idem* at p. 14.
86 *Ibidem*.
87 CJEU, *Google Spain v. AEPD and Mario Costeja Gonzalez*, Case C-131/12, 13 May 2014.
88 *Idem* at para. 15.

a data subject has the right to ask for these search results to be delisted.[89] The Court established that the DPD applied to the situation by asserting that a search engine was a data controller that processed personal data, even though such personal data had been published elsewhere by a third party.[90] Further, the Court creatively established territorial jurisdiction over the situation as Google Inc., the US-incorporated parent company, processes the relevant personal data and its subsidiary Google Spain only sells advertising space. The Court found the activities of Google Inc. and Google Spain to be "inextricably linked".[91] It considered selling advertising space to constitute data processing "in the context of the activities of an establishment of the controller on the territory of a Member State", thus satisfying the DPD's applicable law provision.[92]

To further illustrate that parts of EU data protection law could exemplify the objective territoriality principle, it is useful to recall the responsibilities of data controllers and processers. The data controller is responsible for and controls the data processing; the processer acts upon the instructions of the controller. It is therefore the data controller, as opposed to the processor, that is liable for a data protection breach.[93] Again, the distinction between entities and the associated allocation of responsibility is not as straightforward as the DPD's provisions would suggest.[94] Nonetheless, the law *prima facie* suggests that an act is initiated by a controller, wherever it is located, and terminated by a processor. If that processor is located in the Union, EU data protection law applies to that processing activity, even though the controller that could be located in a third State is responsible for that processing. The GDPR broadens the possibility of making an extraterritorial link as it applies to an establishment of both a controller or a processor in the Union, rather than simply an establishment of the controller, as in the DPD.

A somewhat ambiguous provision in the DPD states that the Directive applies if a data controller is not established on EU territory, but makes use of equipment on Member State territory to process personal data.[95] "Making use" is premised on (i) the activity of the controller and (ii) its clear intention to process personal data.[96] The Article 29 Working Party understands "equipment" to mean "means" because this is a more accurate translation of the same word in non-English versions, it is used in other parts of the Directive and it appears in earlier proposals for the Directive.[97] The Working Party's interpretation is perhaps too broad as the fact that other articles in the Directive and earlier proposals use "means" whilst Article 4(1)c specifically and consciously uses "equipment" suggests they are not comparable terms.

The Article 29 Working Party has nevertheless acknowledged that its broad interpretation of "equipment" could mean the Directive applies "where the processing in question has no real connection with the EU/EEA".[98] A controversial example is when external controllers use cookies or JavaScript banners to collect personal data about EU internet users. For instance, if a data controller located on third State territory, such as a cloud computing service provider in the US, makes use of means on EU territory, by installing cookies that collect data about users' browsing habits, Article 4(1)c would trigger the application of relevant parts of the DPD.[99] The service provider could be obliged

89 *Idem* at at para. 20.
90 *Idem* at at para. 41.
91 *Idem* at at para. 56.
92 *Idem* at at para. 60.
93 Art. 29 WP 2010 (n 74), p. 17.
94 Kuner (n 43) pp. 69-73.
95 DPD, Art. 4(1)c.
96 See the Working Party's Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites (WP 56).
97 Art. 29 WP 2010 (n 74) p. 20.
98 *Idem* at p. 29.
99 NB: a cloud computing service provider is sometimes considered a data processor and sometimes a data controller depending on how it uses personal data; Art. 29 WP's working document on determining the international application of EU DP law to personal data processing on the Internet by non-EU based web sites (WP 56), p. 10 f.

to adhere to certain EU data protection principles that might not apply or could conflict with the third State's laws. For instance, the provider could be compelled to provide users with information on how their personal data are processed and stored. This far-reaching application of the DPD, however, has been understandably controversial, and is generally considered unacceptable.[100] Even the Article 29 Working Party has acknowledged the potential undesirable consequences of this interpretation, for instance EU law applying when a controller outside the EU uses means in the EU to process personal data of non-EU residents.[101] That said, the view that this interpretation is justified because it avoids legal lacunae and protects a fundamental right for EU residents is increasingly popular.[102] The European Charter of Fundamental Rights formally enshrines the right to data protection in a constitutional document.[103] Especially since the Charter became legally binding in 2009, has this pro-protection stance, which supports the wide application of the DPD, gained legal strength.

To fit Article 4(1)c DPD into either the subjective or objective territoriality model, it is useful to ask whether EU data protection law would apply only to data processing that happens in the EU or to the third State controller for all processing stages, including, for example, eventual storage of browsing data by the controller in a third State. If it only applied to data processing in the EU, the article would be seen as more akin to the objective territoriality model of jurisdiction: jurisdiction could only be exercised *vis-à-vis* the processing acts in the EU. As asserted above, data processing upon the instruction of an external controller can be understood as the termination of an act. The Article 29 Working Party, however, is of the view that, because the protection of personal data is a fundamental right, the Directive should apply to the whole processing procedure, including that which happens in a third State.[104] The Working Party, however, does limit this to situations where the connection to the EU is "effective and not tenuous (such as by almost inadvertent, rather than intentional, use of equipment in a Member State)".[105] As explored below, the GDPR could offer clarification of what intentional use of equipment covers, namely targeting or offering of services, or monitoring behaviour.

The third point on national law applicable in the DPD, Article 4(1)b, appears to provide plainly for public international law to give guidance on when EU data protection rules should apply when controllers are located in third States. In practice, however, it simply means that the DPD's provisions apply at embassies abroad, aboard ships, on aeroplanes and similar, according to general public international law and specific treaties.[106] This provision is largely comparable in the DPD and GDPR. The other provisions differ notably, as the following explores.

4.3(b) In the General Data Protection Regulation

The GDPR replaces the use of equipment criterion with a clause that could admit of a potentially wider application of jurisdiction than in the DPD. The GDPR will apply to data processing by external controllers of the personal data of data subjects in the Union when the processing is related to: (i) the offering of goods or services to the data subjects, regardless of whether they require a

100 Moerel, Lokke, ´The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to the Processing of Personal Data of EU Citizens by Websites Worldwide?', *International Data Privacy Law*, Vol. 1, No. 1, 2011, pp. 28-46, p. 29; Maier, Bernhard, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?', *International Journal of Law and Information* Technology, Vol. 18(2), 2010, pp. 142-175, p. 161.

101 Art. 29 WP 2010 (n 74) p. 21.

102 Moerel (n 99) p. 29: "[This interpretation is] fully understandable or even commendable from a protection point of view"; Art. 29 WP 2010 (n 74) p. 24, pp. 31-32; many Data Protection Authorities also support this interpretation.

103 Charter of Fundamental Rights of the European Union (OJ C 364 of 18 December 2000), Art. 8.

104 Art. 29 WP 2010 (n 74) p. 24.

105 *Ibidem*.

106 Svantesson (n 34) pp. 98-99 (citations omitted).

payment; or (ii) the monitoring of these data subjects' behaviour in the EU.[107] The enhanced potential for the GDPR to apply extraterritorially foreseen in Article 3(2) GDPR represents a "dramatic shift from a country of origin to a country of destination approach".[108] This country of destination approach draws parallels with the objective territoriality principle. It has been suggested that this article enables application of the GDPR to all processing of EU residents' personal data, "regardless of a lack of a geographical nexus to the controller or its equipment".[109] The relevant GDPR principles would therefore apply to almost all third State data controllers that process the personal data of data subjects in the EU, which is certainly an example of regulatory overreaching.[110] It is evidently yet to be seen how this article will be applied in practice.

There has been some speculation as to how the GDPR's territorial scope article could apply. Although the Article 29 Working Party opinion on applicable law was written before the GDPR was first drafted, it discusses the notion of targeting as an additional criterion for when a data controller is located outside EU territory.[111] A form of this targeting requirement is now found in Article 3(2) a GDPR. The Working Party affirms there must be an "effective link between the individual and a specific EU country" when a data processing act is aimed at targeting specific individuals.[112] To determine how sufficient this link is, the Working Party suggests following the example of consumer protection law, which is comparable in this situation.[113] One could consider whether a website displays information in an EU language; advertises products and services available in the EU; delivers products or services in the EU; or premises access to a service on the use of an EU credit card.[114]

Similarly, the Rome I Regulation on the law applicable to contractual obligations could offer some guidance here, although it involves "directed activity" and the present article refers to processing activities related to the offering of goods or services, or the monitoring of behaviour, which might not explicitly involve directed activity.[115] Activities related to offering goods or services likely include more activities than directed activity does. In Rome I, a website's accessibility, language and currency does not constitute directed activity.[116] Rather, the website should explicitly attract and solicit visits and sales by, for instance, carrying out local activities in Member States, such as advertising in that State or showing search results on local search engines.[117] The Council of the European Union has asserted that Article 3 GDPR would apply where it was apparent that "the controller is envisaging doing business with data subjects" residing in the Union, which draws parallels with the targeting approach in the Rome I Regulation.[118]

107 GDPR, Art. 3(2).

108 White Paper Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation Omer Tene, Senior Fellow Christopher Wolf, Founder and Co-Chair The Future of Privacy Forum January 2013, p. 2.

109 *Idem* at p. 3, *cit.* Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7 0025/2012 – 2012/0011(COD)), Committee on Civil Liberties, Justice and Home Affairs, Rapporteur: Jan Philipp Albrecht.

110 *Ibidem*.

111 Art. 29 WP 2010 (n 74) p. 24.

112 *Idem* at p. 31.

113 *Ibidem*.

114 *Ibidem*.

115 Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the law applicable to contractual obligations (Rome I), recital 25; see too CJEU, joined cases *Pammer v Reederei Karl Schlüter GmbH & KG11* and *Hotel Alpenhof GesmbH v Oliver Heller* (C 585/08 and C 144/09), judgement of 7 December 2010.

116 Rome I (n 114), recital 24.

117 Moerel (n 99), p. 45, fn 87 *cit.* Rome I (n 114).

118 Council of the European Union, 'Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) – Partial General Approach on Chapter V', 28 May 2014 *available at* http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT, p. 7 para. 20.

Svantesson, however, submits that this focus on "targeting" has disadvantages and imagined benefits.[119] He suggests it would be ineffective when applied *de facto* as the GDPR could be interpreted to "target" and thus apply to all or no States.[120] If targeting were the approach, it would need serious refinement.[121] Nonetheless, if Article 3(2) GDPR were to be interpreted in line with EU consumer protection law, territoriality would still be important to establish what constitutes local activities, that is, Member State-centric activities. If a combination of the Rome I criteria, the Working Party 29 criteria and the Council of the European Union's suggestions could develop into a form of guidance as to when EU data protection principles would apply to a data controller, no matter its location, this could provide for a strong, or at least a less tenuous, connection to trigger jurisdiction.

4.4. Effects Doctrine

The effects doctrine is a particularly controversial basis for enacting extraterritorial jurisdiction.[122] It is an extension of the objective territoriality principle. Some States purport to apply this doctrine when the effects of conduct by citizens abroad, even non-nationals of the affected State, are felt within a State.[123] Thus far, it has mostly been applied by the US and then usually in antitrust cases.[124] The effects doctrine is commonly said to have been introduced in antitrust case *United States v Aluminum Co of America*, where the US Federal Court found that "it is settled law […] that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends".[125] It also appears in an early form in US Supreme Court case *Strassheim v Daily*, which in the context of a federation asserts that "[a]cts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a state in punishing the cause of the harm as if he had been present at the effect if the state should succeed in getting him within its power".[126] The latter poses requirements of intention and effect. According to the US Third Restatement of Foreign Relations Law jurisdiction, the effects doctrine may only apply where extraterritorial conduct has substantial effects on US territory, and where its exercise of jurisdiction is reasonable.[127]

4.4(a) In EU Data Protection Law

Parts of Article 4 DPD on national law applicable could be construed as manifestations of the effects doctrine, indeed most scholars in the field support this opinion.[128] Svantesson suggests the DPD's use of equipment provision and the GDPR's clause on monitoring behaviour of EU residents both fall within the effects doctrine, in that external conduct has an effect in the specific jurisdiction of the EU.[129] He asserts that Article 4 DPD falls into both the objective territoriality principle and the effects doctrine.[130] Kuner asserts that, whilst *prima facie* appearing to fall exclusively within

119 Svantesson, Dan Jerker B., 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation', *International Data Privacy Law*, Vol. 5(4), 2015, pp. 226-234, abstract.

120 *Idem* at p. 232.

121 *Idem* at abstract.

122 See, e.g., the international reaction to *Rio Tinto Zinc Corp v Westinghouse Electric Corp* [1978] 1 ALL ER 434 (HL), where US law was applied to non-US companies in the absence of intra-territorial conduct.

123 Samie, Najeeb, 'The Doctrine of "Effects" and the Extraterritorial Application of Antitrust Laws', *Lawyer of the Americas*, Vol. 14, No. 1 (1982), pp. 23-59, p. 23 (citations omitted).

124 The effects doctrine is arguably developing in EU antitrust law: Scott, Joanne, 'The New EU "Extraterritoriality"', *Common Market Law Review*, Vol. 51(5), 2014, pp. 1343, 1380, 1356, 1358. Scott refers to the EU Merger Regulation, Reg. 139/2004 on the control of concentrations between undertakings, and the EU Derivatives Regulation, Reg. 648/2012 on OTC derivatives, central counterparties and trade repositories.

125 US Federal Court, *United States v Aluminum Co of America* 148 F 2d 416 [2nd Cir 1945).

126 US Supreme Court, *Strassheim v Daily*, 221 US 280.

127 US Third Restatement (n 3) §§ 402-403. See also, Kamminga (n 33) p. 500.

128 See discussions in Svantesson (n 34) and Kuner (n 27) - to a certain degree; see, too, Colonna (n 40) p. 211.

129 Svantesson (n 34) pp. 141-142.

130 Svantesson (n 34) p. 142 *cit.* Kuner (n 37) p. 190.

the objective territoriality principle, the use of equipment clause in the DPD can also be understood as coming under the effects doctrine.[131] This is because the article aims to prevent data controllers from escaping the reach of EU law by establishing themselves outside EU territory.[132]

The issue with the effects doctrine is, whereas it is quite straightforward to differentiate between an act being initiated by a controller and carried out by a processer, thus triggering a form of territoriality jurisdiction, it is more difficult to decipher where an effect of data processing is felt. In the transatlantic context, is an effect felt on EU territory and did all the relevant conduct take place in the US? Did the US data controller have the intention for such effects to occur? It is also difficult to quantify how substantial or detrimental this effect is, and who gets to make that decision. These questions are better applied to concrete examples of conflicts in jurisdiction, rather than to provisions of the DPD and GDPR, which would be merely speculative.

Furthermore, in data protection law, it is challenging to establish a genuine link between an act abroad and an effect. Schultz asserts that in the cybersphere, the link between a State and an act or omission needs to reach a higher threshold than in the physical world.[133] This is due to the fact that everyone with internet access could in theory access every website, indiscriminately establishing this act-effect link. As such, the effects doctrine in respect of data protection law has been criticised as being too open-ended.[134] Such a potentially broad reach of EU data protection law is echoed in the CJEU's pronouncements in the *Lindqvist* judgement.[135] Going farther, Schultz suggests that the effects doctrine "should *a fortiori* be rejected entirely on the Internet".[136] Moreover, if the effects doctrine is an expansion of the objective territoriality principle, and the effects doctrine is so heavily criticised, it is more readily acceptable to consider Article 4 DPD and Article 3 GDPR as constituting the objective territorial principle.[137] In sum, this research considers the DPD and GDPR not to fall under the effects doctrine as easily as other scholars might suggest.

With reference to the targeting approach discussed *supra*, Svantesson calls for a departure from territoriality as the main criterion from which to assess claims to exercise jurisdiction.[138] An approach less connected to territory resonates better with the effects doctrine than with the objective territorial principle. Extrapolating this, if territory in itself is no longer sufficient to demarcate the EU's exercise of jurisdiction over situations with a foreign element, personality-based jurisdictional principles could offer an alternative option, as explored below.

5. Personality

There is arguably a small but perceptible shift from territory to personality as a basis for jurisdiction in EU data protection law. This is especially true in view of the changing nature of State obligations and the increased emphasis on individuals *viz.* data subjects in the GDPR. Classic personality-based jurisdiction law is not based on legal obligations of the State towards individuals, but rather on bonds of allegiance between the individual and the State. Increasingly, however, a State can be understood to owe jurisdictional obligations to individuals, rather than simply to States in respect of individuals.[139] A State could owe duties to individuals as both subjects and objects of

131 Kuner (n 37) p. 190.
132 *Ibidem*.
133 Schultz (n 52) p. 815, citations omitted.
134 Kuner (n 37) p. 190, *cit.* Michaels, Ralf, 'Territorial jurisdiction after territoriality' in: Piet-Jan Slot and Mielle Bulterman (eds.), *Globalisation and Jurisdiction*, Kluwer Law International: Alphen aan den Rijn, 2004, pp. 105-130, p. 123 who says that "in a globalized economy, everything has an effect on everything".
135 *Bodil Lindqvist* (n 58) §71.
136 Schultz (n 52) p. 815, citations omitted.
137 Schultz (n 52) p. 815 *cit.* Currie, John H., *Public International Law*, Irwin Law: Toronto, 2001, p. 301.
138 Svantesson (n 118) pp. 233-234.
139 Mills (n 1) abstract, pp. 27-28, 43.

regulation. As subjects, they are active agents, positive actors and rights-bearers; as objects, they are passive addressees.[140] These concepts operate on a spectrum, not a clear-cut dichotomy.[141] We can conceive of individuals as "international legal persons".[142] With individuals becoming a focus of international rules of jurisdiction, we now turn to individuals in EU data protection law. 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. This raises the question of how personal data can be connected to EU residents as individuals, and how these individuals could invoke classic principles of jurisdiction.

5.1. Individuality and Personality

The protection of personal data has always been connected closely with an individual. Personal data is any information pertaining to an identified or identifiable natural person, who *per se* is a data subject.[143] The full titles of the DPD and GDPR mention not data protection or data privacy, but "the protection of individuals with regard to the processing of personal data".[144] In a broader sense, privacy can be attached to the concepts of individuality and autonomy.[145] Autonomy, in turn, can be understood as being intimately linked to freedom and self-determination.[146] Self-determination and privacy flow ultimately from human dignity. Human dignity is a value upon which the EU is founded and is common to EU Member States.[147] There are strong ties between individuality and developing one's personality; the right to protection of personal data, as a subset and counterpart to the right to privacy, is a personality right.[148] We have a right to informational self-determination, to know and determine what is done with our personal data.

An individual's personal data is closely connoted with an individual as a legal person. Personality-based jurisdiction is also tied to a person's individuality, nationality and personality. This is relevant for extraterritorial jurisdiction because someone's personal data is often controlled, processed and stored in multiple jurisdictions, much more than an actual physical person might be involved in different jurisdictions. As such, someone's personal data could potentially trigger a form of personality jurisdiction.

Whilst this would fulfil the aim of protecting an EU citizen's fundamental right to data protection, it could constitute regulatory overreaching. This overreach could lead to jurisdictional tensions with, most prominently, the US. Indeed, there does still need to be a territorial connection to limit almost universal application of EU data protection laws, but personality is gaining importance in the data protection field.

140 *Idem* at p. 33.
141 *Idem* at p. 27, fn 111.
142 *Idem* at p. 34, fn 136 *cit.* "States have had to concede to ordinary human beings the status of subjects of international law, to concede that individuals are no longer mere objects, mere pawns in the hands of states". –Sohn, Louis B., 'The New International Law: Protection of the Rights of Individuals Rather Than States', *American University Law Review*, 1982, Vol. 32(1).
143 DPD, Art. 2(a).
144 DPD and GDPR full titles.
145 González Fuster (n 64) p. 23 (citations omitted).
146 *Idem* at p. 23 fn 13 *cit.* De Hert, Paul, and Serge Gutwirth. 'Privacy concerns', in Security and Privacy for the Citizen in the Post-September 11 Digital Age: A prospective overview, Report to the European Parliament Committee on Citizens' Freedoms and Rights, Justice and Home Affairs (LIBE), Institute for Prospective Technological Studies, 2003, p. 95.
147 "The Union is founded on the values of respect for human dignity […] and respect for human rights […] These values are common to the Member States" - Consolidated Version of the Treaty on European Union [2008] OJ C115/13, Art. 2.
148 González Fuster (n 64) p. 23 *cit.* Edelman, Bernard, *La personne en danger*, Presses Universitaires de France: Paris, 1999, p. 509.

5.1(a) Active Personality

According to the active personality principle, a State has the right to extend the application of its laws to its nationals outside its territory.[149] This principle is commonly a basis for criminal jurisdiction. It can also extend to companies, ships and aircraft.[150] A common example is when a State prosecutes its citizen who commits a crime abroad. There are no examples in EU data protection law that readily lend themselves to the active personality principle.

5.1(b) Passive Personality: in general

The passive personality principle covers situations where a State exercises jurisdiction over injured nationals abroad.[151] It is usually applied in criminal law cases to enable jurisdiction over victims. The passive personality principle is arguably the most hard-line basis for exercising extraterritorial jurisdiction and has thus been much challenged.[152] Whilst under customary international law the passive personality principle is not usually considered a valid basis to permit the exercise of extraterritorial prescriptive jurisdiction,[153] recent State practice suggests States might be more accepting of the principle.[154] Indeed, in reinterpreting existing permissive principles to see how data protection law fits into them, passive personality is an increasingly useful concept to delineate the EU's regulatory authority.

5.1(c) Passive Personality: in EU Data Protection law

EU residents are rights holders and potential victims of having their right to personal data protection violated when their personal data is transferred, controlled or processed outside of EU territory. Especially in the cybersphere, it is important to note that an EU resident's right to data protection could conceivably be violated "even in absence of any detriment to the affected individual".[155] Indeed, an individual could be legally, but not physically, present.[156] As such, every data subject could be a potential victim and could unwittingly suffer an interference in his or her fundamental right to data protection.

5.1(c)(i) Data Protection Directive

Article 29 Working Party has acknowledged the potential unsatisfactory consequences of understanding cookies and JavaScript banners as "equipment" on EU territory and consequently triggering the application of the DPD.[157] It posits that this interpretation could result in EU law applying when a controller outside the EU uses means in the EU to process personal data of non-EU residents.[158] As highlighted *supra*, the Working Party supports the application of the DPD to non-EU controllers processing data by means in the EU. This view suggests the Working Party takes

149 See Lowe, Vaughan and Staker, Vaughan, 'Jurisdiction', in Evans, Malcom D, *International Law*, 3rd ed., OUP: Oxford, 2010, p. 322.
150 Kamminga (n 33).
151 *Idem* referring to *Arrest Warrant* (n 16).
152 See Kuner (37) p. 188.
153 Currie (n 29) p. 36.
154 Svantesson (n 34) p. 141 *cit.* Ireland-Piper, Danielle, 'Extraterritorial criminal jurisdiction: Does the long arm of the law undermine the rule of law?', *Melbourne Journal of International Law*, Vol. 13(1), pp. 1-36, pp. 13-14, which discusses Australian law and Gillian D Triggs' scholarship on the matter.
155 Milanovic, Marko, 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age', *Harvard International Law Journal*, 2015, Vol. 56(1), pp. 81-146, p. 134 *cit.* ECtHR, *Huvig v. France*, App. No. 11105/84, 24 April 1990, para. 35.
156 Ford, Richard T., 'Law's Territory' (A History of Jurisdiction), *Michigan Law Review*, Vol. 97(4), 1999, pp. 843-930, p. 904.
157 Art. 29 WP 2010 (n 74) p. 21.
158 *Ibidem*.

issue specifically with the law applying to *non-EU residents*. Accordingly, to lessen such undesirable effects, an additional criterion for applying jurisdiction would plausibly be personality, that is, nationality or, most probably, residency. EU residents are highly likely to be citizens of an EU country, so the personality principle hinged purely upon someone's nationality could apply. This research equates personality in the personality principle with either citizenship or residency because EU data protection law refers to data subjects residing in the EU, not their citizenship. This also evades the exclusion of non-EU nationals who live in the EU, to whom EU data protection law ought to apply according to the principle of non-discrimination. Furthermore, by virtue of its status as a fundamental right, the application of the right to data protection does not depend on citizenship.[159]

The residence approach would permit EU data protection principles to apply to an EU resident's personal data regardless of its location.[160] Residence is similar to the private international law concept of domicile, which gives the individual, as opposed to the State, some freedom to choose jurisdiction.[161] Indeed, private international law rules on adjudicative jurisdiction recall personality jurisdiction.[162] We focus on residency as opposed to citizenship because it would be excessive to expect EU data protection law to apply, for example, to the personal data of an Italian citizen who resides in Australia if his or her banking data were exchanged between Australian and Chinese financial institutions. Indeed, whilst the EU Charter affirms the right to data protection for "everyone", EU Data Protection Authorities ordinarily attend to EU data protection legal claims where the data subject to EU link is strong.[163] As the Article 29 Working Party confirms in its guidelines on implementing the *Google Spain* judgement, a data subject's residency in an EU Member State often qualifies as a strong link.[164]

The Article 29 Working Party has also posited that it would be unacceptable to protect only those *residing* in the EU as the fundamental right to data protection is enjoyed without discriminating based on someone's nationality or residence.[165] This statement is problematic for several reasons. In the transatlantic context, it raises issues because data protection is a fundamental right recognised in the legally-binding EU Charter on Fundamental Rights, but is not recognised as a fundamental right in the US legal system.[166]

A specific example of how an EU Data Protection Authority, in this case the Greek one, has extended the applicability of its data protection law shows how form of the passive personality principle has been applied in an EU-third State dimension.[167] The Greek Data Protection Authority required that data controllers outside Greece who processed the personal data of Greek residents appoint a representative in Greece, who would be accountable for this data processing.[168] The European Commission took issue with this requirement, so Greece changed their law in 2006.[169] This draws parallels, however, with certain substantive rules in the GDPR that could apply very broadly. Svantesson has called the potential situation where a non-EU organisation that has little contact

159 The DPD and GDPR acknowledge that rules on data processing should respect a person's fundamental rights and freedoms, whatever that person's nationality or residence (DPD, recital 2; GDPR, recital 2).

160 Kuner (n 27) pp. 238-239 and see p. 239, fn. 161 *cit.* Bygrave, Lee, 'Determining applicable law pursuant to European Data Protection Legislation' (2000) 16 *Computer Law and Security Report*, p. 256 as making this argument. Bygrave draws parallels between this approach and existing EU consumer protection applicable law rules.

161 Mills (n 1) p. 21.

162 "In the rules of adjudicatory jurisdiction in civil and commercial matters under private international law, the domicile principle may serve as a variation on the active personality principle" – Ryngaert (n 6) p. 108.

163 Art. 29 Working Party, "Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12", 14/EN WP 225, 26 November 2014, para. 19.

164 *Ibidem*.

165 Art. 29 WP 2010 (n 74) p. 24.

166 See, EU Charter (n 102) Art. 8.

167 Kuner (n 37) pp. 188-189.

168 *Idem* at p. 189 (citations omitted).

169 *Ibidem*.

with EU residents is obliged to implement certain measures, such as appointing a data protection officer in accordance with the GDPR, "absurd". [170] Indeed, this notion runs counter to the Greek example above, and could, as Svantesson suggests, discredit the GDPR.[171]

5.1(c)(ii) General Data Protection Regulation

The DPD's scope of application refers only to the "processing of personal data", without mentioning data subjects or EU residents.[172] In contrast, the GDPR focuses more on individuals. It applies to the processing of "personal data of data subjects who are in the Union […] the offering of goods or services […] to such data subjects in the Union [or] the monitoring of their behaviour [as long as it takes place] within the Union".[173] The DPD appears to anchor jurisdiction more palpably on territory and the GDPR seems to take more of a personality-based approach. That is not to say physical territory is inconsequential in the GDPR. A subject's location if being offered goods or services, or being monitored, is still important. Companies can often, but not always, use geo-location technology to determine a data subject's location. This raises questions of how the GDPR would apply if a subject's location could not be determined; whilst not currently a pertinent issue, this situation could be conceivably solved with a focus on personality. Svantesson is also of the view that the GDPR's applicability provisions appear to fall within the passive personality principle, or at least a version thereof.[174]

The GDPR's scope article has been interpreted as lending itself to the potential overextended application of EU data protection law through emphasising the personality/residence requirement. The GDPR could conceivably apply to all data collection and processing pertaining to data subjects in the Union, with no requirement for the location of a controller or equipment to establish a territorial nexus. This expansive interpretation could "bring about precisely the 'general application' that the ECJ tried to prevent [in the *Lindqvist* case]".[175] However, this interpretation might not be so expansive as residence or location implies a territorial connection: the GDPR lends itself readily to jurisdiction based on residence or location of the data subject, which is linked to territory *and* an individual. The residence or domicile view has been gaining greater traction with the popular focus on protecting individuals.[176] In national and international legal practice, to link residence with nationality or personality to permit the exercise of personality-based jurisdiction is not a new approach.[177] The GDPR, however, has evolved. Whereas the territorial scope article used to refer to "data subjects residing in the Union", it now reads "data subjects who are in the Union", which *prima facie* seems to broaden its reach even more by removing an explicit residency requirement.[178]

170 GDPR, Arts. 37-39; Svantesson (n 118) p. 31.
171 *Idem* at p. 31.
172 DPD, Art. 4(1).
173 GDPR, Art. 3(2).
174 Svantesson (n 34) pp. 141-142.
175 White Paper (n 107) p. 3, *cit.* Draft Report on the proposal for GDPR.
176 "One could also argue that the place of the domicile [or residence of the data subject] should be the place of jurisdiction, in order to give maximum protection to the individual" – Kuner (n 27), pp. 238-239 *cit.* Bygrave, Lee A., 'Determining Applicable Law pursuant to European Data Protection Legislation', *Computer Law & Security Report* (now *Computer Law & Security Review*), 2000, Vol. 16(4), pp. 252–257, p. 256 (The problem of more than one State's laws governing the same situation "could be remedied if applicable law were to be made the law of the State in which a data subject has his/her domicile. Such a rule would parallel existing European rules on jurisdiction and choice of law in the case of consumer contracts"); "Perhaps the artificiality of attempting to localize internet conduct territorially means that jurisdiction should be determined by reference to the defendant's nationality or the claimant's domicile?" – Bigos, Oren, 'Jurisdiction over Cross-Border Wrongs on the Internet', *International and Comparative Law Quarterly*, Vol. 54(3), 2005, pp. 585-620, p. 602 (citations omitted). For EU legislation on jurisdiction and consumer protection that takes a similar approach, see 1968 Brussels Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters, Arts. 13–15; 1988 Lugano Convention on Jurisdiction and the Enforcement of Judgements in Civil and Commercial Matters, Arts. 13– 15; Rome I, (n 114), Art. 5, Recital 25.
177 Referencing Dutch and Belgian law, see Ryngaert, Cedric, 'Amendment of the Provisions of the Dutch Penal Code Pertaining to the Exercise of Extraterritorial Jurisdiction', *Netherlands International Law Review*, Vol. 61(2), pp 243-248, p. 245 (citation omitted).
178 *Cf.* COM(2012) 11 final 2012/0011 (COD), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 25.1.2012, Art. 3(2) to GDPR, Art. 3(2).

That said, other sections of the GDPR related to its territorial scope mention a data subject's residence on EU territory.[179] In practice, residence could be a useful jurisdictional hook and location is certainly important.

Whilst not an EU privacy instrument, the Asia-Pacific Economic Cooperation Framework (APEC) provides for something close to the passive personality principle and draws certain parallels with, for instance, the adequacy requirement in EU data protection law.[180] In that Framework, the national data protection laws of the APEC Member State where the original data controller collected the relevant personal data attach to and follow that data, even when transferred abroad.[181] As the transfer from one State to another implies a territorial connection to a controller or a processor, and to a place of data export or import, the passive personality principle does not *per se* apply to the EU data protection framework.[182] There is a necessary territorial connection implied in cross-border data transfers. Further, if territoriality were completely sidelined, the abovementioned targeting requirement in the GDPR could easily lead to problematic regulatory overreach. Whilst personality is becoming a pragmatic basis for the EU's exercise of extraterritorial jurisdiction, it needs to be combined with territorial forms of jurisdiction to be effective in practice. As the GDPR applies "regardless of whether the processing takes place in the Union or not", the residence criterion could be an ideal combination of territory and personality that would most effectively prompt the EU's exercise of prescriptive jurisdiction over situations with a foreign element.

6. Conclusion

Under public international law, a State has a right to exercise jurisdiction. States are expected to show restraint when attempting to regulate a situation with foreign elements. The EU's DPD is far-reaching and has tangible effects beyond its territory. It could apply to third State controllers if the data processing were carried out in the context of the activities of an establishment of the controller on EU territory or if they made use of equipment on EU territory. The GDPR could also apply broadly. It could apply to a third State controller processing data related to the offering of goods or services, or the monitoring of the behaviour, of data subjects in the Union. Both the DPD and GDPR could indirectly prescribe third State data protection law through their adequacy requirements. The foregoing data protection provisions could conceivably fall into the subjective territoriality, objective territoriality, passive personality or effects doctrine. This research concludes that the provisions do not come under any one of these principles, but rather a combination of interpretations of several of them. The DPD and GDPR's applicable law and scope articles could most plausibly constitute the objective territoriality and passive personality principles. Whilst there appears to be a shift from territory to personality in European data protection law, territory is still necessary to trigger the application of jurisdiction. The demarcations provided by public international law could thus offer ways to mitigate transatlantic conflicts in jurisdiction.

179 See, *inter alia*, GDPR, recitals 122 and 124.

180 Asia-Pacific Economic Cooperation, APEC Privacy Framework, APEC#205-SO-01.2.

181 Kuner (n 37) p. 189 *cit.* Asia-Pacific Economic Cooperation, APEC Privacy Framework, APEC#205-SO-01.2, §26.

182 See, Ryngaert, Cedric, 'Whither Territoriality? The European Union's Use of Territoriality to Set Norms with Universal Effects', in: *What's Wrong with International Law?: Liber Amicorum A.H.A. Soons*, Cedric Ryngaert, Erik J. Molenaar and Sarah Nouwen (eds.), Brill Nijhoff: Leiden, 2015, pp. 434-448, p. 441, fn 22 – "Admittedly, one could also make the argument that, insofar as EU law follows the transfer of data of EU persons abroad, the protection offered by EU law is based on the passive personality principle, which allows states to protect the interests of their own citizens abroad. It is noted, however, that a transfer from the EU to another state presupposes an initial EU territorial presence of data".

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.org

N°1 **"The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area"** *(November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)*

N°2 **"The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection"** *(November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)*

N°3 **"Towards efficient cooperation between supervisory authorities in the area of data privacy law"** *(October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)*

N°4 **"The data protection regime in China"** *(November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)*

N°5 **"The right to privacy and personal data protection in Brazil: time for internet privacy rights?"** *(February 2016)by Vinícius Borges Fortes (23 pages)*

N°6 **"Permissions and Prohibitions in Data Protection Jurisdiction"** *(May 2016) by Mistale Taylor (25 pages)*