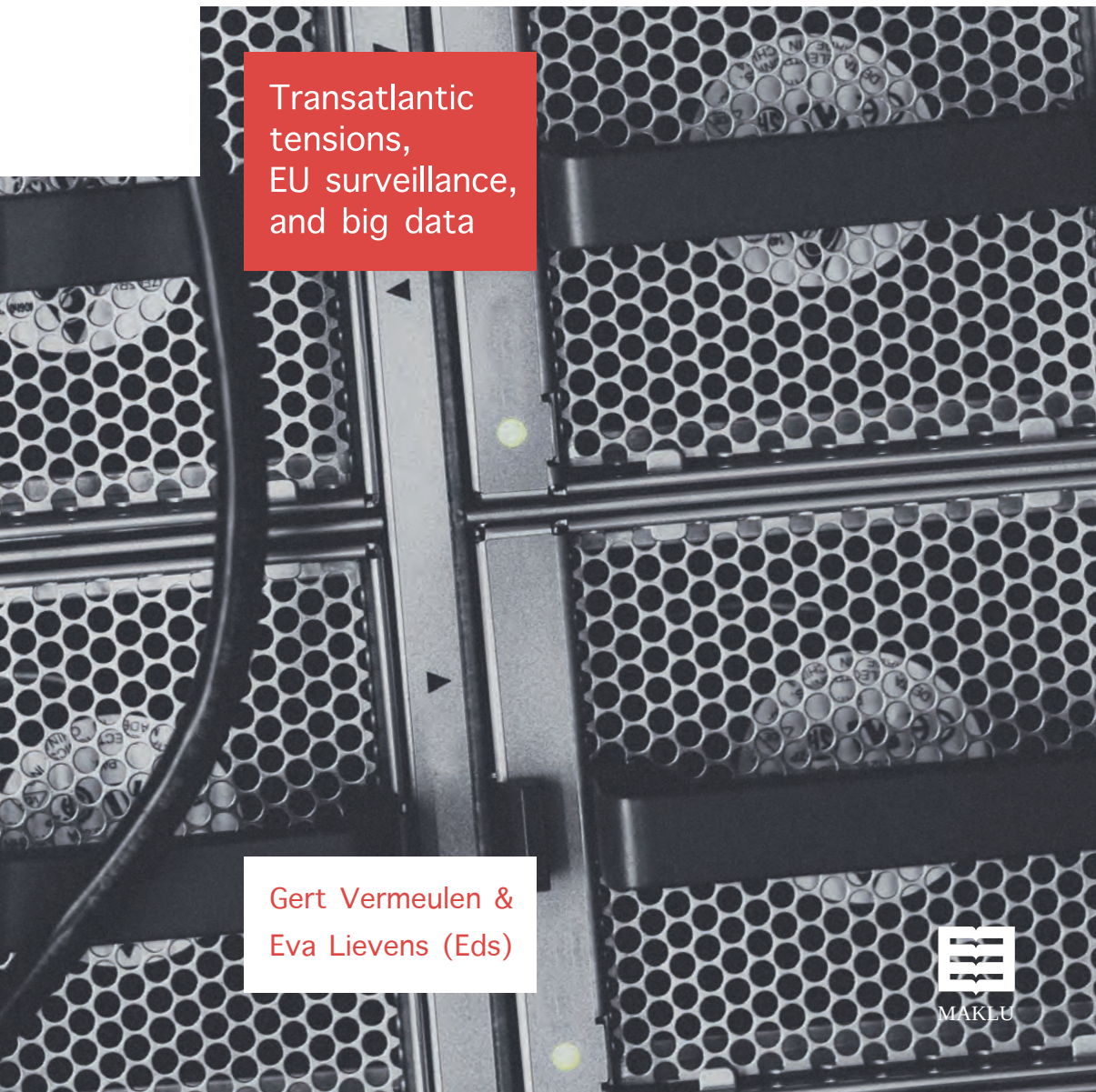
# Data Protection and Privacy under Pressure



Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen &
Eva Lievens (Eds)

MAKLU

# Data Protection and Privacy under Pressure

Transatlantic tensions, EU surveillance, and big data

Gert Vermeulen
Eva Lievens
(Eds)

**Maklu**

Antwerp | Apeldoorn | Portland

Data Protection and Privacy under Pressure
Transatlantic tensions, EU surveillance, and big data
Gert Vermeulen and Eva Lievens (Eds)
Antwerp | Apeldoorn | Portland
Maklu
2017

341 p. – 24 x 16 cm
ISBN 978-90-466-0910-1
D/2017/1997/89
NUR 824




Maklu-Publishers
Somersstraat 13/15, 2018 Antwerp, Belgium, info@maklu.be
Koninginnelaan 96, 7315 EB Apeldoorn, The Netherlands, info@maklu.nl
www.maklu.eu

USA & Canada
International Specialized Book Services
920 NE 58th Ave., Suite 300, Portland, OR 97213-3786, orders@isbs.com,
www.isbs.com

# Reconciling the (extra)territorial reach of the GDPR with public international law

BRENDAN VAN ALSENOY[1]

## 1. INTRODUCTION

Extraterritoriality and data protection make for a controversial mix. Different attitudes towards privacy, coupled with a lack of global consensus on jurisdictional boundaries, fuel an intense debate among those advocating jurisdictional restraint and those emphasizing the need to ensure effective protection.[2] With the adoption of the General Data Protection Regulation (GDPR),[3] the EU legislature has revised the territorial scope of EU data protection law. In part, the GDPR confirms choices made by policymakers and the Court of Justice of the European Union (CJEU) in the context of Directive 95/46/EC.[4] In other respects, important new elements have been introduced.

During the preparation of the GDPR, commentators warned that the EU was in danger of overstepping its jurisdictional boundaries.[5] As a member of the

---

[1] Legal advisor, Commission for the Protection of Privacy, Belgium; senior affiliated postdoc researcher, KU Leuven Centre for IT & IP law (imec). I would to thank Joelle Jouret and Michal Czerniawski for their useful input and feedback during the writing process. Any errors or mistakes are my own. Email: Brendan.VanAlsenoy@privacycommission.be.

[2] See Dan Jerker B. Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing 2013) 20, 21; Chistopher Kuner, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5 IDPL 235; Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230 and Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567.

[3] Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ L 119/1-88.

[4] Regulation Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31-50.

[5] See eg Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1,10.

international community, the European Union is bound to observe the general principles of customary international law of jurisdiction.[6] According to customary international law, there should be a *bona fide* connection between the subject matter of a dispute and the State asserting jurisdiction over it.[7] The aim of this contribution is to scrutinize the triggers'[8] that render EU data protection law applicable to conduct which takes place, either in whole or in part, outside of Union territory. The analysis shall be limited to the EU's exercise of prescriptive jurisdiction, leaving questions of adjudicative or enforcement jurisdiction for future work. I will begin by analyzing the territorial scope of the GDPR, in particular its potential for extra-territorial reach.[9] Similarities and differences between the GDPR and Directive 95/46 will be highlighted, looking back at relevant case law and guidance to clarify key concepts. Next, the legitimacy of EU's assertion of prescriptive jurisdiction will be assessed from the perspective of public international law. The main question this contribution seeks to answer is: can the (extra-)territorial scope of the GDPR be reconciled with the principles of public international law? Or has it in fact 'overextended' itself?

## 2. THE EXTRA-TERRITORIAL REACH OF THE GDPR

The territorial scope of the GDPR is determined by article 3. For purposes of this contribution, the two most important triggers are (a) the presence of a relevant establishment of a controller or processor on EU territory and (b)

---

[6] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 5, with reference to Case C-366/10 *Air Transport Association of America and Others v Secretary of State for Energy and Climate Change* EU:C:2011:864, paras 101 and 123.

[7] See Cedric Ryngaert, *Jurisdiction in International Law* (Oxford University Press 2008) 21 et seq. See also Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 155.

[8] A "trigger" is a mechanism that launches the application of EU law and delimits its personal and territorial scope of application (Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344).

[9] For a discussion of the concept of "extra-territoriality" see Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 60. See also Joanne Scott, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 Am J Comp L 87, 90.

the monitoring or targeting of EU data subjects.[10] Whilst the first ground governs the situation in which the controller or processor has an establishment on EU territory, the second ground governs the situation where there is no such establishment. It is already clear, however, that both triggers have an extra-territorial dimension.

## 2.1. Article 3(1) GDPR

Article 3(1) provides that the GDPR shall apply

> 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.

Determining the territorial scope of the GDPR pursuant to article 3(1) implies prior identification of the entity which is acting as a 'controller' or 'processor' of the processing, as well as the location of its 'establishment(s)'. Equally important, however, is the reference to the 'context of activities': this criterion implies that the establishment must be involved in activities implying the processing of personal data in question.[11] Or rather, the establishment must be involved in a 'real and effective exercise of activities in the context of which the personal data are being processed'.[12]

Article 3(1) GDPR is the successor of article 4(1)(a) of Directive 95/46, with two notable changes. First, article 3(1) GDPR makes reference not only to an establishment of a controller, but also to an establishment of a processor. As a result, the processing of personal data might also be subjected to EU law by virtue of a *processor* having an establishment located within the EU.[13] Second, article 3(1) explicitly indicates that it is not necessary for the processing of

---

[10] In addition to these 'main criteria', the GDPR also specifies in article 3(3) that the GDPR 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. Recital (25) indicates that this might be the case, for example, as regards the processing of personal data carried out in a Member State's diplomatic mission or consular post.

[11] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

[12] ibid 11.

[13] For a discussion of implications of this addition see Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729, 741 and Lokke Moerel, 'The data transfer regime for processors does not make sense and requires clarification' (*GDPR Conundrums: Data Transfer*, 9 June 2016) <https://iapp.org/news/a/gdpr-conundrums-data-transfer>.

personal data to take place within the EU in order for the GDPR to apply. As a result, article 3(1) GDPR has the potential for extra-territorial reach: EU data protection law shall apply to processing taking place outside EU territory if it is being carried out 'in the context of the activities of an establishment of the controller or processor' located within the EU.[14] To properly delineate the extra-territorial reach of the GDPR, it is necessary to analyze the words 'establishment' and 'in the context of the activities'.

### *2.1.1. 'Establishment'*

The term 'establishment' is not formally defined by the GDPR, but according to recital (22) implies 'the effective and real exercise of activity through stable arrangements.' The legal form of such 'arrangements', whether it be simply a branch or a subsidiary with a legal personality, is not a determining factor in that respect.[15]

The term 'establishment' is not always given a uniform meaning or interpretation in EU law.[16] In relation to the freedom of establishment under article 50 TFEU, the Court of Justice of the European Union has considered that a stable establishment requires that 'both human and technical resources necessary for the provision of particular services are permanently available'.[17] In the context of data protection law, the concept of establishment has received a particularly broad interpretation. In its *Weltimmo* ruling, the Court of Justice of the European Union (CJEU) stated that the concept should be interpreted in a flexible rather than a formalistic manner.[18] It extends to any real and effective activity — even a minimal one — exercised through stable

---

[14] See also Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 107.

[15] This portion of recital (22) GDPR is almost identical to the corresponding text of recital (19) of Directive 95/46.

[16] Scott (n 8) 1352.

[17] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010). See also Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 35 (concluding that all subsidiaries and most branch offices will qualify as 'establishments').

[18] Case C-230/14 *Weltimmo sro v Nemzeti Adatvédelmi és Információszabadság Hatóság* EU:C:2015:639, para 29 (hereafter "*Weltimmo*"). Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' WP 179 (16 December 2015).

arrangements.[19] According to the CJEU, both the degree of stability of the arrangements and the effective exercise of activities should be assessed in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.[20] As a result, in some circumstances, the presence of *one single representative* can suffice to constitute a stable arrangement if that representative acts with a sufficient degree of stability 'through the presence of the necessary equipment for provision of the specific services concerned in the Member State in question'.[21]

Although it has received a broad interpretation, the concept of establishment is not without limits. Mere accessibility of a website, for example, would not suffice to constitute an 'establishment' for purposes of article 3(1).[22] A stable presence of at least some human and technical resources appears necessary to conclude that an 'establishment' exists within the EU.[23]

### *2.1.2. 'In the context of the activities'*

Mere physical presence of a controller or processor on Union territory is not sufficient to render the GDPR applicable pursuant to article 3(1). To render the GDPR applicable, it is necessary that the processing at issue is undertaken "in the context of the activities" of an establishment on EU territory. The CJEU has clarified the meaning of the words 'in the context of the activities' in three rulings: *Google Spain*, *Weltimmo* and *Verein für Konsumenteninformation*.

In *Google Spain*, the CJEU was asked to determine whether Google's search engine activities (ie, the crawling of web pages, indexation, storage, etc) may be viewed as taking place 'in the context of the activities' of one of its local subsidiaries, *Google Spain SL. Google Spain's* activities consisted in the promotion and sale of advertising space, as a commercial representative of Google. The CJEU began by confirming that the notion of 'in the context of the activities' does not require that the establishment in question itself is actively

[19] *Weltimmo* (n 18).

[20] *Weltimmo* (n 18).

[21] *Weltimmo* (n 18) para 30. See also the Opinion of Advocate General Cruz Villalón on *Weltimmo* (n 18) para 34.

[22] Case C-191/15 *Verein für Konsumenteninformation v Amazon EU Sàrl* EU:C:2016:388, para 76 (hereafter "*Verein für Konsumenteninformation*").

[23] See also Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

engaged in the processing.[24] It also considered that those words cannot be interpreted restrictively, in the light of the objective of ensuring effective and complete protection.[25] The CJEU went on to consider that the activities of the search engine operator and those of its establishment are 'inextricably linked', as Google's search engine service is closely related to the activity of selling advertising space.[26] Specifically, the Court reasoned that

> the activities relating to the advertising space constitute the means of rendering the search engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.[27]

Based on these considerations, the CJEU concluded that the processing of personal data is carried out 'in the context of the activities' of an establishment of the controller

> when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which *orientates its activity towards the inhabitants of that Member State*.[28]

*Weltimmo* concerned the processing of personal data by a company running a property dealing website. Although the company was formally registered in Slovakia, it published adverts concerning Hungarian properties.[29] For that purpose, it processed the personal data of the advertisers, several of whom had Hungarian nationality. When the Hungarian Data Protection Authority decided to investigate, *Weltimmo* countered that the authority was not competent and could not apply Hungarian law in respect of a supplier of services established in another Member State.[30] In its assessment, the CJEU reiterated

---

[24] Case C-131/12 *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* EU:C:2014:317, para 52 (hereafter: "*Google Spain*").

[25] *Google Spain* (n 24) para 53.

[26] *Google Spain* (n 24) para 56.

[27] *Google Spain* (n 24) para 56.

[28] *Google Spain* (n 24) para 60 (emphasis added).

[29] *Weltimmo* (n 18) para 9.

[30] *Weltimmo* (n 18) para 12.

that the wording 'in the context of the activities' cannot be interpreted restrictively, with reference to its earlier *Google Spain* ruling.[31] To ascertain whether the establishment was involved in the exercise of activities 'in the context of which' the processing is carried out, the referring court was invited to take into account the fact that the activity of the controller in respect of the processing is 'mainly or entirely directed at that Member State'.[32] In addition, the referring court was invited to consider the presence of a representative in that Member State, who is responsible for *recovering the debts resulting from that activity* and for *representing* the controller in the administrative and judicial proceedings relating to the processing of data concerned.[33] The nationality of the persons concerned by the data processing was, however, deemed irrelevant.[34]

In *Verein für Konsumenteninformation*, the CJEU was asked to clarify whether or not the processing of personal data by *Amazon EU* must comply with the data protection rules of each Member State to which its commercial activities are directed.[35] While indicating that mere accessibility of a website does not suffice to constitute a relevant 'establishment', the Court clearly hinted that there may be an establishment other than *Amazons EU*'s Luxembourg headquarters in the context of which the processing of personal data is being carried out.[36] If the referring court found that to be the case, the processing of personal data by *Amazon EU* would be governed by the law of the Member State to which it directs its activities.[37] The CJEU left it to the referring court, however, to determine whether there is indeed an establishment on the territory of a Member State other than Luxembourg in the context of which the processing of personal data is taking place.[38]

---

[31] *Weltimmo* (n 18) para 25.

[32] *Weltimmo* (n 18) para 41. To establish whether the activities of the controller were in fact 'mainly or entirely' directed at Hungary, the referring court was invited to consider whether the advertisements on the property dealing website concerned properties situated in Hungary and whether they were written in the Hungarian language.

[33] *Weltimmo* (n 18) para 41.

[34] *Weltimmo* (n 18) para 41.

[35] *Verein für Konsumenteninformation* (n 22) para 72.

[36] *Verein für Konsumenteninformation* (n 22) para 80.

[37] *Verein für Konsumenteninformation* (n 22) para 81.

[38] *Verein für Konsumenteninformation* (n 22) paras 81 and 79.

### *2.1.3. Evaluation*

The case law of the CJEU concerning Directive 95/46 clearly favors a broad interpretation of the notions of 'establishment' and 'in the context of the activities'. With the adoption of article 3(1) GDPR, the EU legislator has chosen to confirm the CJEU's broad interpretation of these concepts.[39] While fa stable presence of at least some human and technical resources appears necessary in order to qualify as an 'establishment', the permanent presence of a single agent equipped with little more than a laptop may be enough, at least in some circumstances.[40] The notion of 'in the context of activities' has similarly received a broad interpretation. It is not required that the personal data are processed 'by' the establishment in question or that the controller itself resides on EU territory. There must, however, exist a clear link between the processing at issue and the activities of the establishment. The link can be direct (eg a customer support activity) or indirect (eg monetization activities which enable and cause the processing to be performed).[41] It is interesting to note, however, that the CJEU has repeatedly referred to the *orientation of activities* when determining applicable law. In each of the aforementioned cases, the CJEU considered whether the establishment in question 'orientates' or 'directs' its activities to the Member State in question. Such orientation seemingly takes precedence over 'degree of involvement': while it has been

[39] See also Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230, 237; Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3,13 and Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 575.

[40] The Opinion of Advocate General Cruz Villalón on *Weltimmo* (n 18) para 34.

[41] The statement that the link may be indirect does not imply that the link may be attenuated. Indeed, while the link between the processing activity and the activities of the establishment may be considered as 'indirect', the CJEU took care in *Google Spain* to emphasize that the activities of the establishment and the processing at issue were 'inextricably' linked. See also Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in *Google Spain'* WP 179 (16 December 2015). Gömann, on the other hand, considers that the *Google Spain* ruling has effectively interpreted article 4(1)a so extensively that it is enough if there is "*a somewhat tangible physical establishment on EU territory whose supporting activity shows at least a tiny (online) link to the actual processing activity of the third country processor*") (Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 574). See also Maja Brkan, *Data Protection and European Private International Law* (EUI Working Papers, RSCAS 2015/40, 2015) 33.

suggested that the territorial scope of Directive 95/46 should be determined by looking at which establishment has a 'closer connection' to the processing,[42] the CJEU has so far only had regard to (a) the relationship between the processing at issue and the activities of the establishment and (b) whether the establishments directs those activities to the territory of an EU Member State.[43]

## 2.2. **Article 3(2) GDPR**

Article 3(2) explicitly addresses the territorial scope of the GDPR in case of processing of personal data by a controller or processor not established in the Union. It provides that the GDPR shall be applicable 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.

### *2.2.1. 'Data subjects in the Union'*

While article 3(2) only applies in case the controller or processor is not established in the Union, the processing of personal data must concern data subjects located in the Union. De Hert and Czerniawski offer the example of a European tourist shopping on Fifth Avenue in New York as a situation where article 3(2) GDPR clearly would not apply.[44] The requirement that the data subject be located in the Union must be assessed at the moment when the relevant trigger activity takes place, ie at the moment of offering of goods or

---

[42] Opinion of Advocate General Saugmandsgaard Øe on *Verein* (n 22) para 127.

[43] See also Opinion of Advocate General Bot, Case C-2010/16, 24 October 2017, para 100 (considering that every establishment may be relevant, regardless of whether there is a European 'head office', which within the group's internal division of tasks is considered "exclusively responsible" for collecting and processing personal data throughout the entire territory of the European Union). The judgment of the CJEU in this procedure is still pending.

[44] Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230, 238.

services or the moment when the behavior which is being monitored. Processing activities which are 'related' to the activity which triggered application of article 3(2) also falls within the territorial scope of the GDPR.

### *2.2.2. 'Offering of goods or services'*

The first activity triggering the application of article 3(2) is the 'offering of goods or services'. Recital (23) clarifies that article 3(2)(a) requires conduct on the part of the controller or processor which demonstrates its *intention* to offer goods or services to data subjects located in the Union:

> In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is *apparent* that the controller or processor *envisages* offering services to data subjects in one or more Member States in the Union [emphasis added].

As a result, mere accessibility of a website is considered insufficient to ascertain such an intention.[45] Conversely, use of a currency or language generally used in one or more EU Member States, in particular where that language is not generally used in the third country where the controller or processor is established, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.[46]

The criteria identified in recital (23) echo the CJEU's reasoning in the joined *Pammer* and *Hotel Alpenhof* cases.[47] Here, the CJEU was called upon to clarify what it means to 'direct activity' within the meaning of article 15(1) of the Rome I Regulation.[48] While the notions of 'directing activity' and 'offering of goods and services' are not identical[49], the CJEU's case law on this point is likely to be influential in shaping the further interpretation of article

---

[45] Recital 23.

[46] ibid (n 45).

[47] Joined cases C-585/08 and C-144/09 *Peter Pammer v Reederei Karl Schlüter GmbH & Co KG and Hotel Alpenhof GesmbH v Oliver Heller* EU:C:2010:740 [2010] ECR I-2527, paras 84 and 94.

[48] Regulation No 593/2008 on the law applicable to contractual obligations (Rome I), [2008] OJ L-177/6-16.

[49] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 17.

3(2)(a).[50] In the *Pammer* and *Hotel Alpenhof* ruling, the CJEU also identified other factors as being relevant, such as: the payment of money to a search engine to facilitate access by consumers domiciled in various Member States; the mention of telephone numbers with the international code; the top-level domain name used; and the description of itineraries from one or more other Member States to the place where the service is provided.[51]

### *2.2.3. 'Monitoring of behavior'*

The second activity triggering the application of article 3(2) is 'monitoring of behaviour'. Recital (24) indicates that article 3(2)(b) is first and foremost concerned with online tracking and profiling activities:

> In order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are *tracked on the internet* including potential subsequent use of personal data processing techniques which consist of *profiling* a natural person, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.

Article 3(2)(b) GDPR is the successor of article 4(1)(c) of Directive 95/46, that provides that Member States must apply their national data protection laws if the controller who is not established in the EU 'makes use of equipment' situated on its territory. While the term 'equipment' in first instance refers to physical objects,[52] the Article 29 Working Party has given the term

---

[50] See also Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 585.

[51] *Pammer* (n 47) paras 81 and 83. See also Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1,7 and Ruth Boardman, James Mullock and Ariane Mole, *Bird & Bird guide to the General Data Protection Regulation* (april 2016) 2.

[52] Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 227. The legislative history of Directive 95/46 suggests that its drafters only had physical objects in mind when using the word 'equipment'. See also Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 33 and 36.

a broad interpretation, which comprises both human and technical resources.[53] More specifically, the Working Party understands the term 'equipment' to have the same meaning as the term 'means' used in article 2(d) of the Directive (ie the definition of controller).[54] On the basis of this broad interpretation, the Working Party has considered that the use of JavaScript banners or cookies might also be considered as 'means' within the meaning of article 4(1)(c).[55] As a result, the use of cookies by non-EU controllers to track data subjects located in the EU is considered to fall within the territorial scope of Directive 95/46. While this interpretation has been the subject of considerable criticism, the EU legislator has apparently chosen to embrace it by providing it with a more explicit legal footing.

Interestingly, neither article 3(2)b nor recital (24) make any reference to the intention of the controller or processor to monitor the behavior of data subjects in the Union. As a result, it would appear that cookie-based tracking of EU data subjects would trigger the territorial scope of the GDPR, regardless of whether the cookie was placed via a website actively targeting EU residents. The only requirement stipulated by article 3(2)(b) is that the monitoring of behavior concerns behavior which takes place in the Union.[56]

Finally, it should be noted that even though recital (24) only refers to 'tracking on the internet', the wording of article 3(2)(b) is sufficiently broad to cover other techniques of behavioral monitoring (eg through wearables or other smart devices).[57]

---

[53] Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010).

[54] ibid (n 53).

[55] ibid 21-22.

[56] See also Anni-Maria Taka, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications' (Master's Thesis in Private International Law and EU Law, Uppsala Universitet 2017) 83 <http://www.diva-portal.org/smash/get/diva2:1127596/FULLTEXT01.pdf> and Paul Voigt and Axel von dem Bussche, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer 2017) 28.

[57] Taka (n 56) 78; Merlin Gömann, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CM L Rev 567, 588 and Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203, 215.

### *2.2.4. Evaluation*

Article 3(2)(a) extends the territorial scope of the GDPR to non-EU controllers and processors which 'target' EU data subjects.[58] The targeting approach subjects the application of EU law to entities located outside its territory to the requirement that those entities reveal the intention to reach ('actively target') individuals located within their territory.[59]

While asserting jurisdiction solely on the basis of targeting is arguably new to EU data protection law[60], the target and direction of offering goods and services has been an important factor in the case law of the CJEU analyzing the territorial scope of EU data protection law.[61] In doing so, article 3(2)(a) incorporates a trigger familiar to other areas of EU legislation, namely the trigger of 'market access' or 'conduct that consists of a step in the direction of gaining access to the EU market'.[62]

Interestingly, article 3(2)(b) does not, at least on the face of it, involve a market access trigger. While the monitoring of behavior may by itself be viewed as involving a form of 'targeting', it does not necessarily involve 'purposeful' targeting of data subjects who are in the Union. For example, websites often place (or enable the placement of) cookies without discriminating on the basis of the geographic origin of the website visitor, ie regardless of whether the

---

[58] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226; Paul de Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 238; Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3,17 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 235.

[59] Thomas Schultz, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 817.

[60] De Hert and Czerniawski (n 58) 238.

[61] Cf *supra*; section II.1.c. See also Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729, 735.

[62] See Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1348 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 230.

visitor's query originates from the EU or not. Such cookies may be used to track individuals' online activities across websites, often with a view to enable online behavioral advertising. If that is the case, are those processing activities covered by article 3(2)(b)? This question will be revisited later on.

In any event, commentators are still divided as to whether the GDPR's increased emphasis on targeting is a good or bad thing. Svantesson considers that targeting has great theoretical appeal, but is often difficult to apply in practice.[63] Both Taylor and Czerniawski consider the overt emphasis on targeting a step forward in comparison to article 4(1)(c) of Directive 95/46, providing a stronger connection to trigger jurisdiction.[64] Kindt, on the other hand, considers the targeting approach as too restrictive and warns that significant gaps in protection may arise in the future.[65]

## 3. ASSESSMENT UNDER PUBLIC INTERNATIONAL LAW

Under public international law, there must be a 'sufficient connection' before a state can assert either prescriptive or adjudicative jurisdiction.[66] There are approximately five general principles upon which a jurisdictional claim might be based, namely (1) the territoriality principle (objective and subjective); (2) the nationality principle (active or passive); (3) the effects principle; (4) the protective principle; or (5) the universality principle.[67] For purposes of public international law, it is the territoriality principle which is the primary - but not the sole - basis of jurisdiction.[68] The principle of territoriality entails

---

[63] Dan Jerker B. Svantesson, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226.

[64] Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 18 and Michal Czerniawski, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 232.

[65] Els J. Kindt, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CM L Rev 729, 738-739.

[66] Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 IJLT 176.

[67] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 80; Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 143.

[68] Uta Kohl, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* (Cambridge University Press 2007) 20; Cedric Ryngaert, *Jurisdiction in International*

that each state has the right to regulate persons, matters and events within its own territory.[69] It is based on the principle of sovereign equality of States and the principle of non-intervention.[70] A corollary of the territoriality principle is that states should exercise some restraint before asserting jurisdiction extra-territorially: if a state wishes to be recognized as sovereign within its own borders, it must respect the sovereignty of other states within their borders.[71] Nevertheless, states increasingly undertake to regulate conduct taking place abroad, using a variety of justifications for doing so.[72] The EU is no exception in this regard.[73] The aim of this section is to scrutinize the extraterritorial reach of the GDPR from the perspective of public international law.

## 3.1. Establishment: A physical or virtual connection with EU territory?

Article 3(1) of the GDPR advances the 'establishment' of a controller or processor on EU territory as a trigger for the application of EU data protection law. 'Establishment' is normally a strong connecting factor. In theory, all this concept does is provide for a straightforward application of the territoriality principle.[74] If you are established and operate within a state's territory, you

*Law* (Oxford University Press 2008) 27 et seq. See also Section 402 of the *Third Restatement of the Law of the Foreign Relations Law of the United States*.

[69] Kohl (n 68) 89.

[70] Ryngaert (n 68) 29.

[71] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL105, 108. Other arguments advocating against extra-territorial assertions of jurisdiction include unforeseeability, limited enforceability, liability under multiple jurisdiction, etc. See eg Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142, 161-162.

[72] Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 61; Uta Kohl, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* 89-108; Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344; Robert Dover and Justin Frosini, *The extraterritorial effects of legislation and policies in the EU and US* (Study for the European Parliament's Committee on Foreign Affairs 2012) 48.

[73] See in particular Joanne Scott, 'The New EU 'Extraterritoriality'' (2014) 51 CM L Rev 1343, 1344.

[74] Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18 IJLIT 142, 174.

have to play by its rules. This makes sense. However, things may get trickier when the territorial nexus of establishment is used as a means to regulate conduct abroad. Moerel has already pointed out that in the case of article 4(1)(a) of Directive 95/46, the principle of territoriality has a 'more or less virtual nature'.[75]

> The formal place of establishment of the controller is not relevant […] The controller of the data itself may be established outside of the EU. […] [T]he territoriality principle is in fact adhered to by Article 4(1)(a) as *the data processing is virtually connected to the territory of the EU* (ie takes place in the context of the activities of the establishment in the Member State).[76]

So the use of 'establishment' to link the processing with EU territory may not be entirely straightforward. There are, however, additional justifications that might solidify the EU's assertion of jurisdiction vis-à-vis non-EU entities. The effects principle, which is an extension of the territoriality principle, stipulates that states may regulate behavior which takes place outside its territory insofar as it produces substantial effects within its territory.[77] This principle is frequently applied in competition matters, whereby states use it to assert jurisdiction over foreign practices which restrict competition in national markets.[78] Even though the effects principle has been developed in the context of antitrust law,[79] its logic can be extended to other areas of law, including data

---

[75] Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28, 29.

[76] Moerel (n 75) 29-30 (emphasis added). See also Paul De Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 234.

[77] Section 402 of the Third Restatement of the Law of the Foreign Relations Law of the United States. See also Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 82; Cedric Ryngaert, *Jurisdiction in International Law, United States and European perspectives* (PhD Thesis, Leuven 2007) 198. See also Max Huffman, 'A Retrospective of Twenty-Five Years on the Foreign Trade Antitrust Improvements Act' (2007) 44 Hous LR 285.

[78] Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 82.

[79] See also Deepa Rishikesh, 'Extraterritoriality Versus Sovereignty in International Antitrust Jurisdiction' (1990) 14 World Competition 33, 49; Cf A Retrospective of Twenty-Five Years (43).

protection law.[80] Similar to antitrust law, data protection cannot be fully effective when applied strictly territorially.[81] Moreover, international human rights law offers direct support for the proposition that states should consider the effects of foreign conduct on their citizens' privacy.[82]

In its *Google Spain* ruling, the CJEU made repeated references to the need to ensure 'effective and complete' protection of individuals. It also noted, at several occasions, that the processing of personal data by search engines may bring about a serious interference with the rights which Directive 95/46 was designed to protect.[83] This language suggests that the CJEU's conclusion was motivated in no small part by the recognition that Google's search engine activities may have a real impact (ie 'substantial effect') on data subjects in the EU. In the words of the CJEU:

> […] it cannot be accepted that the processing of personal data carried out for the purposes of the operation of the search engine should escape the obligations and guarantees laid down by Directive 95/46, which would compromise the directive's effectiveness and the effective and complete protection of the fundamental rights and freedoms of natural persons which the directive seeks to ensure […].[84]

The effects principle is considered a controversial basis of jurisdiction, particularly in relation to internet content regulation.[85] Due to the global nature of the internet, any state might claim to be affected by online content or activity originating from anywhere in the world.[86] The jurisdictional principle of *reasonableness* requires states to balance the need for effectiveness against

---

[80] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 109.

[81] See more generally John H. Currie, *Public International Law* (Irwin Law 2001) 300.

[82] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 78 and Mistale Taylor, 'The EU's human rights obligations in relation to its data protection laws with extraterritorial effect' (2015) 5 IDPL 246.

[83] *Google Spain* (n 24) paras 80-81.

[84] *Google Spain* (n 24) para 58.

[85] See generally Daniel Castro and Robert Atkinson, 'Beyond Internet Universalism: A Framework for Addressing Cross-border Internet Policy' (2014) The Internet Technology & Innovation Foundation 1, 7.

[86] See also Jonathan Zittrain, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law' Harvard Law School Public Law Research Paper No. 03/2003.

the principle of non-intervention.[87] The CJEU's interpretation of article 4(1)(a) is quite 'reasonable' if one considers the alternative. If the CJEU had ruled otherwise, this would, in the long run, create an unfair competitive advantage for non-EU based companies (who only have subsidiaries in the EU) over EU companies (who are fully established in the EU). The advantage would be particularly significant in markets where personal data processing is an important aspect. In other words: holding article 4(1)(a) inapplicable would be the equivalent of extending 'special guest status' to foreign data controllers who offer their (data-intensive) services on the EU market.[88] The suggestion that the CJEU is mindful of the potential implications for the EU market is all the more compelling if one considers that the CJEU's holding explicitly refers to whether the establishment in question 'orientates' its activities to the Member State in question.

### 3.2. Is it 'targeting' or 'being targeted' that matters?

Earlier it was pointed out that article 3(2) GDPR employs 'targeting' as a trigger to render the GDPR applicable to controllers and processors not established in the EU. In such a scenario, the primary nexus with EU territory is not the presence of a controller or processor within the EU, but rather the location of the data subjects to which the relevant activities are targeted.[89] Article 3(2) GDPR identifies two such 'relevant activities': the offering of goods or services and the monitoring of behavior. In case of the former, it is clear that the GDPR will only apply if it is apparent that the controller or processor 'purposefully targeted' data subjects within the EU. In case of the latter, the situation is not so clear-cut.

---

[87] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 116. See Restatement (Third) of the Law of the Foreign Relations. The principle of reasonableness is closely linked (but not identical to) the principle of 'comity'. For more information see Jurisdiction in International Law (n 43) 42 et seq. See also Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)', (2010) 18 IJLT 244.

[88] Brendan Van Alsenoy and Marieke Koekkoek, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105, 110.

[89] Clearly Gottlieb, *The General Data Protection Regulation: Key Changes and Implications* (Alert Memorandum 2016) 3 <https://www.clearymawatch.com/wp-content/uploads/sites/106/2016/10/Alert-memo-PDF-Version-2016-50.pdf>.

Asserting jurisdiction in case of purposeful targeting is often viewed as legitimate.[90] While the precise meaning of what constitutes 'targeting' (and what does not) may vary[91], the purposeful targeting arguably does enhance the legitimacy of a state's decision to regulate.[92] If a foreign entity deliberately targets its activity towards residents of another country, it may reasonably foresee that the government of that country might impose certain rules. Moreover, the use of targeting criteria can help to minimize the potential impact on other states' interests in so far as the assertion of prescriptive jurisdiction is limited to activity which are targeted to its own inhabitants.[93]

While the requirement of 'purposeful targeting' is absent from article 3(2)(b) GDPR, one could argue that such a requirement should be 'read into' this provision. First, it has been suggested that some degree of intentionality is in fact implicit in the concept of 'monitoring' itself.[94] Second, the legislative history of article 3(2) GDPR suggests that the EU legislature precisely sought to soften the potential for global applicability of the GDPR.[95] On the other hand, one could argue if the EU legislature had wanted to subject the monitoring trigger of article 3(2)(b) GDPR to the requirement of 'purposeful targeting', it would have done so. Moreover, if article 3(2)(b) GDPR were to require "purposeful" targeting of people in the EU, its practical importance would be significantly

---

[90] See eg Omer Tene and Christopher Wolf, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013) 1, 6-8.

[91] Thomas Schultz, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface' (2008) 19 EJIL 799, 816.

[92] Also Paul De Hert and Michal Czerniawski, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 238-239.

[93] This is not to say that States may never undertake to regulate behavior which is not specifically targeted at their jurisdiction or its inhabitants, it merely serves underscore that the potential with other States interests will be considerably smaller the scope of the jurisdictional assertion is limited to activities targeted at the State's own territory.

[94] See also Anni-Maria Taka, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications', citing R. Jay, Guide to the General Data Protection Regulation: A Companion to Data Protection Law and Practice, 75-76.

[95] See Dan Jerker B. Svantesson 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 107-110.

reduced: such processing activities would often be covered by article 3(2)(a) GDPR.

The two opposing viewpoints are likely to lead to the same conclusion in relation to companies who specialize in online tracking. These companies amass vast amounts of data on people located within the EU, which is often specifically intended to facilitate personalized (ie 'targeted') advertising of people located in the EU. As such, there is a clear intention to 'target' people located in the EU. But what about the individual websites who enable third parties to track cookies? According to the Article 29 Working Party, website operators ('publishers') bear some responsibility when enabling of targeted advertising.[96] However, these website operators do not necessarily themselves monitor the behavior of data subjects across websites. While they do perform processing activities 'related' to the monitoring of data subjects in the Union (by enabling third parties to track visits to their website), some might argue that the connection with EU territory becomes too attenuated.

Perhaps a balanced outcome might be reached applying a systematic reading of article 3(2) GDPR and its corresponding recitals. Recital (24) explicitly refers to internet tracking and profiling techniques, suggesting either that an element of intentional or active tracking is required,[97] or that the monitoring must reach a certain level of intrusiveness. The benefit of such an approach would be that it still enables some form of case-by-case assessment. Moreover, such an approach would be more readily justifiable under the effects principle, which stipulates that a State may regulate behavior what takes place outside its territory insofar as it produces 'substantial effects' within its territory.

[96] Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' WP 171 (22 June 2010). The distribution of responsibility between publishers and ad network providers may be clarified in the context of CJEU Request for a preliminary ruling from the Oberlandesgericht Düsseldorf (Germany) lodged on 26 January 2017 - Case C-40/17 *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* [2017] action brought on January 26, 2017.

[97] Rob Sumroy and others, 'New rules, wider reach: the extra-territorial scope of the GDPR' (*Slaughter and May*, June 2016) <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>.

## 4. CONCLUSION

When reviewing the extraterritorial reach of the GDPR, it is clear that article 3 reflects a combination of jurisdictional principles.[98] Where its applicability is triggered by virtue of an establishment of the controller or processor, the extraterritorial reach can be justified by a combination of the territoriality principle and the effects principle. As the case law of the CJEU indicates that the 'orientation' of activities is significant, the need to ensure a level playing field within the EU market helps to argue that the EU's exercise of prescriptive jurisdiction is in fact reasonable.

The targeting approach of article 3(2) GPDR can also be justified by reference to the objective territoriality and/or effects principle.[99] As far as the offering of goods or services is concerned, the additional criteria set forth by the GDPR help to protect against jurisdictional overreach. Where the monitoring of data subjects in the EU is concerned, however, no specific safety valves are provided for. In my opinion, applicability of the GDPR can be readily justified once the monitoring activity reaches a certain level of intrusiveness. In the absence of further clarification, however, considerable uncertainty remains as to when exactly article 3(2)(b) will be triggered. It is therefore desirable that that this matter be clarified either in future regulatory guidance or by the EU legislature as part of its review of the ePrivacy Directive. The pending reference before the CJEU regarding the geographical scope of delisting may also provide further insight.[100] In any event, it will be interesting to see to what extent principles of public international law will effectively be taken into account when determining the extra-territorial scope of EU data protection law.

---

[98] See also Liane Colonna, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203, 213-215.

[99] See also Mistale Taylor, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3, 18-24, who additionally cites the personality principle as a principle of jurisdiction underlying the GDPR's approach.

[100] Request for a preliminary ruling from the Conseil d'État (France) lodged on 21 August 2017, Case C-507/17 *Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*.

## 5. SELECTED LITERATURE

Article 29 Data Protection Working Party, 'Opinion 2/2010 on online behavioural advertising' WP 171 (22 June 2010)

Article 29 Data Protection Working Party, 'Opinion 8/2010 on applicable law' WP 179 (16 December 2010)

Article 29 Data Protection Working Party, 'Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain' WP 179 (16 December 2015)

Boardman R, Mullock J and Mole A, *Bird & Bird guide to the General Data Protection Regulation*, (april 2016)

Brkan M, *Data Protection and European Private International Law* (EUI Working Papers, RSCAS 2015/40, 2015) 33

Castro D and Atkinson R, 'Beyond Internet Universalism: A Framework for Addressing Cross-border Internet Policy' (2014) The Internet Technology & Innovation Foundation 1

Colonna L, 'Article 4 of the EU Data Protection Directive and the irrelevance of the EU–US Safe Harbor Program?' (2014) 4 IDPL 203

Currie JH, *Public International Law* (Irwin Law 2001)

Czerniawski M, 'Do We Need the 'Use of Equipment' as a factor for the territorial applicability of the EU Data Protection Regime?' in Dan Jerker B. Svantesson and Dariusz Kloza (eds), *Trans-atlantic data privacy as a challenge for democracy* (Intersentia 2017) 221, 227.

De Hert P and Czerniawski M, 'Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context' (2016) 6 IDPL 230

Dover R and Frosini J, *The extraterritorial effects of legislation and policies in the EU and US* (Study for the European Parliament's Committee on Foreign Affairs 2012)

Gömann M, 'The new territorial scope of EU data protection law: deconstructing a revolutionary achievement' (2017) 54 CML Rev 567

Gottlieb C, *The General Data Protection Regulation: Key Changes and Implications* (Alert Memorandum 2016) 3 <https://www.clearymawatch.com/wp-content/uploads/sites/106/2016/10/Alert-memo-PDF-Version-2016-50.pdf>

Huffman M, 'A Retrospective of Twenty-Five Years on the Foreign Trade Antitrust Improvements Act' (2007) 44 Hous LR 285.

Kindt EJ, 'Why research may no longer be the same: About the territorial scope of the New Data Protection Regulation' (2016) 32 CLS Rev 729

Kohl U, *Jurisdiction and the Internet – Regulatory Competence of Online Activity* (Cambridge University Press 2007)

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 1)' (2010) 18 IJLT 176

Kuner C, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18 IJLT 244

Kuner C, 'Extraterritoriality and regulation of international data transfers in EU data protection law' (2015) 5 IDPL 235

Maier B, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet' (2010) 18 IJLIT 142

Moerel L, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1 IDPL 28

Moerel L, 'The data transfer regime for processors does not make sense and requires clarification' (*GDPR Conundrums: Data Transfer*, 9 June 2016) <https://iapp.org/news/a/gdpr-conundrums-data-transfer>

Rishikesh D, 'Extraterritoriality Versus Sovereignty in International Antitrust Jurisdiction' (1990) 14 World Competition 33

Ryngaert C, *Jurisdiction in International Law* (Oxford University Press 2008)

Ryngaert C, *Jurisdiction in International Law, United States and European perspectives* (PhD Thesis, Leuven 2007)

Schultz T, 'Carving Up the Internet: Jurisdiction, Legal Orders, and the Private /Public International Law Interface' (2008) 19 EJIL 799

Scott J, 'The New EU 'Extraterritoriality'' (2014) 51 CML Rev 1343

Scott J, 'Extraterritoriality and Territorial Extension in EU Law' (2014) 62 Am J Comp L 87

Sumroy R, 'New rules, wider reach: the extra-territorial scope of the GDPR' (*Slaughter and May*, June 2016) <https://www.slaughterandmay.com/media/2535540/new-rules-wider-reach-the-extraterritorial-scope-of-the-gdpr.pdf>

Svantesson DJB, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing 2013)

Svantesson DJB, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical Justification and Its Practical Effect on U.S. Businesses' (2014) 50 Stan J intl L 60

Svantesson DJB, 'Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation' (2015) 5 IDPL 226

Taka A-M, 'Cross-Border Application of EU's General Data Protection Regulation (GDPR) – A private international law study on third state implications' (Master's Thesis in Private International Law and EU Law, Uppsala Universitet 2017)

Taylor M, 'Permissions and prohibitions in data protection jurisprudence' (2016) 2 Brussels Privacy Hub Working Paper 3

Tene O and Wolf C, *Overextended: Jurisdiction and Applicable Law under the EU General Data Protection Regulation* (White Paper, The Future of Privacy Forum, 2013)

Van Alsenoy B and Koekkoek M, 'Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted''(2015) 5 IDPL 105

Voigt P and von dem Bussche A, *The EU General Data Protection Regulation (GDPR) - A Practical Guide* (Springer 2017)

Zittrain J, 'Be Careful What You Ask For: Reconciling a Global Internet and Local Law', Harvard Law School Public Law Research Paper No. 03/2003

Since the Snowden revelations, the adoption in May 2016 of the General Data Protection Regulation and several ground-breaking judgments of the Court of Justice of the European Union, data protection and privacy are high on the agenda of policymakers, industries and the legal research community.

Against this backdrop, *Data Protection and Privacy under Pressure* sheds light on key developments where individuals' rights to data protection and privacy are at stake. The book discusses the persistent transatlantic tensions around various EU-US data transfer mechanisms and EU jurisdiction claims over non-EU-based companies, both sparked by milestone court cases. Additionally, it scrutinises the expanding control or surveillance mechanisms and interconnection of databases in the areas of migration control, internal security and law enforcement, and oversight thereon. Finally, it explores current and future legal challenges related to big data and automated decision-making in the contexts of policing, pharmaceutics and advertising.

Gert Vermeulen is full professor of international and European criminal law and director of the Institute for International Research on Criminal Policy (IRCP) at Ghent University, and privacy commissioner at the Belgian DPA.

Eva Lievens is assistant professor of law and technology at Ghent University.

www.maklu.eu
isbn 978-90-466-0910-1