Article 4(1)(a) 'establishment of the controller' in EU data privacy law - time to rein in this expanding concept?

Svantesson, Dan Jerker B

Published in:
International Data Privacy Law

DOI:
10.1093/idpl/ipw013

Published: 01/01/2016

Document Version:
Peer reviewed version

Article 4(1)(a) "establishment of the controller" in EU data privacy law – time to rein in this expanding concept?

Dan Jerker B. Svantesson*

Abstract

- Article 4(1)(a) of Directive 95/46/EC plays an important role in determining the applicability of EU data privacy law. However, its wording lends itself to various interpretations.
- Consequently, it is unsurprising that Article 4(1)(a) has been the object of several recent CJEU judgments, and that this provision is the object of ongoing litigation.
- This article seeks to analyse and predict the future landscape by examining the two relevant recent CJEU decisions (the *Google Spain* case and the *Weltimmo* case), Advocate General Saugmandsgaard Øe's Opinion in *Verein für Konsumenteninformation*, and in particular the currently ongoing *Facebook Fanpages* dispute.

1. Introduction

Article 4 of the Data Protection Directive – defining the Directive's territorial scope – has always been shrouded in a veil of mystery.[1] No one seems to have been quite certain as to exactly what the role of that Article is and how it relates to other provisions; especially how it relates to Article 28 dealing with jurisdiction. For the first 15 years or so, the confusion surrounding Article 4 seems to have mattered little in that, whatever issue Article 4 was to address, that issue did not get much time in the limelight.

That has now changed, not least due to the Internet. Article 4 has been the very focal point in one recent CJEU decision (*Weltimmo*[2]), and an important matter in another recent CJEU decision (*Google Spain*[3]). Furthermore, the proper interpretation of Article 4 is one of several important matters in a request to the CJEU for a preliminary ruling from the

* Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia). Visiting Professor, Faculty of Law, Masaryk University (Czech Republic). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council. Once again, Radim Polčák has provided useful input on an earlier draft, and in addition, the author is grateful to have had the opportunity to discuss a draft version of this article with members of Facebook's legal team. All views, and mistakes, are those of the author alone.

[1] See e.g.: Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014), p. 199, and Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2nd ed, 2007) 111-112.

[2] C-230/14.

[3] C-131/12.

Oberster Gerichtshof of Austria (*Verein für Konsumenteninformation*[4]), in relation to which Advocate General Saugmandsgaard Øe delivered his Opinion on 2 June 2016. And Article 4 is set to again be the battle ground in the CJEU, namely in the context of the ongoing dispute relating to Facebook's so-called 'Fanpages'.[5] Amongst these disputes, it is particularly subsection 1(a) – processing of personal data in the context of the activities of an establishment of a controller in the Union – that has been the focal point, and it is the meaning of that specific subsection I will discuss here.

Importantly, since Article 3 of the forthcoming Regulation – which plays the role Article 4 does for the Directive – adopts largely the same focus on processing of personal data in the context of the activities of an establishment of a controller (or a processor) in the Union, the CJEU's decisions in *Weltimmo*, *Google Spain, Verein für Konsumenteninformation* and the *Facebook Fanpages* case, do not only determine current law; they set important precedents for the future operation of the Regulation.

In light of that, this article seeks to analyse and predict the future landscape by examining the two relevant recent CJEU decisions, Advocate General Saugmandsgaard Øe's Opinion in *Verein für Konsumenteninformation*, and in particular the currently ongoing *Facebook Fanpages* dispute.

2. The Directive's Article 4(1)(a) and the Regulation's Article 3(1)

In some previous issues of this journal, I have criticised the more directly 'extraterritorial' dimensions of the Directive's Article 4 and the Regulation's Article 3.[6] Here, however, we can restrict ourselves to only examining Article 4(1)(a) of the Directive and Article 3(1) of the Regulation, both of which deals with entities established within the EU:

> **Article 4(1)(a) of the Directive**
>
> 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; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.[7]
>
> **Article 3(1) of the Regulation**

[4] C-191/15.
[5] C-210/16.
[6] Dan Svantesson, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, *International Data Privacy Law* (2015) 5(4); pp. 226-234 and Dan Svantesson, A "layered approach" to the extraterritoriality of data privacy laws, *International Data Privacy Law* (2013) 3(4); pp. 278-286.
[7] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data* 1995 OJ (L 281), Article 4(1)(a).

> 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.[8]

The similarity between Article 4(1)(a) of the Directive and Article 3(1) of the Regulation are obvious; but then so too are the differences. Most strikingly, while Article 4(1)(a) of the Directive specifically addresses situations where the same controller is established on the territory of several Member States, Article 3(1) of the Regulation does not do so (for reasons discussed below).

3. What we learnt from *Google Spain*

The procedural background of the *Google Spain* case would be well-known to every reader of this journal and I will not repeat it here. In fact, in an earlier issue of this journal, I have partly analysed the *Google Spain* case from the perceptive of what it tells us about the operation of Article 4.[9] Thus, here it suffices to – in the briefest terms – repeat the key implications of the *Google Spain* case as they relate to Article 4(1)(a).[10]

Essentially, the reason the *Google Spain* case gave rise to Article 4 considerations was due to the fact that Google – as it had done with success previously in both Australia[11] and New Zealand[12] – argued that the local branch of Google (in this case, Google Spain) being within the reach of the local law did not automatically mean that the US-based Google Inc, that actually operates the company's well-known search engine, would be. The CJEU concluded the following:

> In the light of that objective of Directive 95/46 and of the wording of Article 4(1)(a), it must be held that the processing of personal data for the purposes of the service of a search engine such as Google Search, which is operated by an undertaking that has its seat in a third State but has an establishment in a Member State, is carried out 'in the context of the activities' of that establishment if the latter is intended to promote and sell, in that Member State, advertising space offered by the search engine which serves to make the service offered by that engine profitable.
>
> In such circumstances, the activities of the operator of the search engine and those of its establishment situated in the Member State concerned are inextricably linked since the activities relating to the advertising space constitute the means of rendering the search

[8] http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.
[9] Dan Svantesson, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, International Data Privacy Law (2015) 5(4); pp. 226-234.
[10] For a valuable analysis of how the CJEU approach Article 4(1)(a) in this matter see e.g.: Brendan Van Alsenoy and Marieke Koekkoek, Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted' International Data Privacy Law (2015)5 (2): 105-120, pp. 106-111.
[11] *Duffy v Google INC & Anor* [2011] SADC 178.
[12] *A v Google New Zealand Ltd* [2012] NZHC 2352.

> engine at issue economically profitable and that engine is, at the same time, the means enabling those activities to be performed.[13]

While this statement does not lack clarity in the context it was presented, we will have reason to analyse it in detail below, not least in the context of its potential implications for the *Facebook Fanpages* case.

4. What we learnt from *Weltimmo*

Decided on 1 October 2015, the CJEU's important decision in the *Weltimmo* case was somewhat overshadowed by the CJEU's 6 October 2015 decision invalidating the Safe Harbour scheme.[14] At any rate, the dispute stemmed from a fine imposed on a Slovakian company (Weltimmo s. r. o.) by the Hungarian data protection authority (*Nemzeti Adatvédelmi és Információszabadság Hatóság*).

The *Kúria* (i.e. the Supreme Court of Hungary) referred eight questions to the CJEU. For the *Kúria's* six first questions – the questions of relevance here – the key issue was the correct meaning of the term 'establishment'. In that context, the Court noted that, while the owner resides in Hungary, Weltimmo is registered in Slovakia and is therefore established there within the meaning of company law. However, importantly, Weltimmo carried out no activity in Slovakia but had representatives in Hungary. Weltimmo had opened a bank account in Hungary and had a letter box there for its everyday business affairs. The property website which constituted its main business was written exclusively in Hungarian and dealt only with properties in Hungary.

All this suggests that Weltimmo has a substantial connection to Hungary and that Hungary has a legitimate interest in the matter. It also suggests that the actual link to Slovakia – the place of registration – was comparatively weak. Consequently, it may be seen as unsurprising that the Court held that Weltimmo pursues a real and effective activity in Hungary, and the Court stressed the need for a flexible definition of the concept of 'establishment', rather than a formalistic approach whereby undertakings are established solely in the place where they are registered. Against this background, the CJEU concluded that:

> Article 4(1)(a) […] must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out;[15]

Expanding upon this point, the CJEU also noted that:

[13] *Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González* (Case C-131/12) [55]-[56].
[14] C-362/14.
[15] *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Case C-230/14), at para. 41.

> [I]n order to ascertain, in circumstances such as those at issue in the main proceedings, whether that is the case, the referring court may, in particular, take account of the fact (i) that the activity of the controller in respect of that processing, in the context of which that processing takes place, consists of the running of property dealing websites concerning properties situated in the territory of that Member State and written in that Member State's language and that it is, as a consequence, mainly or entirely directed at that Member State, and (ii) that that controller has 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 the data concerned;[16]

The Court added that, "by contrast, the issue of the nationality of the persons concerned by such data processing is irrelevant."[17]

5. What we are learning from the *Verein für Konsumenteninformation* case

The dispute between the Austrian consumer protection association (*Verein für Konsumenteninformation*) and Amazon EU Sàrl (Amazon EU) is a consumer protection matter which raises complex private international law questions straddling both Regulation (EC) No 593/2008 on the law applicable to contractual obligations (Rome I)[18] and Regulation (EC) No 864/2007 on the law applicable to non-contractual obligations (Rome II).[19] Importantly for our context, it also tackles the interpretation of Article 4(1)(a) of the Directive. The dispute stemmed from Amazon EU's use of a choice of laws clause nominating Luxembourg law also for Austrian consumers – an approach the Austrian consumer protection association considered to contravene EU law. One of the questions referred to the CJEU is:

> 4.2. Is the processing of personal data by an undertaking that in the course of electronic commerce concludes contracts with consumers resident in other Member States, in accordance with Article 4(1)(a) of 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, and regardless of the law that otherwise applies, governed exclusively by the law of the Member State in which the establishment of the undertaking is situated in whose framework the processing takes place or must the undertaking also comply with the data protection rules of those Member States to which its commercial activities are directed?[20] (internal footnote omitted)

[16] *Ibid*.
[17] *Ibid*. For a deeper analysis of the Weltimmo decision, see e.g.: Dan Svantesson, The CJEU'S *Weltimmo* Data Privacy Ruling – Lost in the Data Privacy Turmoil, Yet So Very Important, Maastricht Journal of European and Comparative Law 23(2) (2016); pp. 332-341.
[18] OJ [2008] L177/6.
[19] OJ [2007] L199/40.
[20] Request for a preliminary ruling from the Oberster Gerichtshof (Austria) lodged on 27 April 2015 — Verein für Konsumenteninformation v Amazon EU Sàrl (Case C-191/15).

At the time of writing, we are yet to see how the CJEU approaches this matter. However, Advocate General Saugmandsgaard Øe delivered his Opinion on 2 June 2016. His reasoning is clear and his propositions sensible. Thus, the CJEU ought to follow his lead.

First of all, Advocate General Saugmandsgaard Øe adopted the view that Amazon EU being registered in Luxembourg, combined with its lack of a subsidiary in Austria, does not, in itself, preclude, the conclusion that that Amazon may have an establishment in Austria.[21] At the same time, he stressed that, the fact that Amazon EU comes into contact with and enter into contracts with Austrian consumers via its German language website does not, of itself, mean that Amazon EU is established in Austria.[22] All this is of course in line with *Weltimmo*.

Even more significantly, Advocate General Saugmandsgaard Øe noted important differences between the *Verein für Konsumenteninformation* matter and *Google Spain*:

> Apart from other differences as to the factual circumstances, there is a difference between the matter that gave rise to that judgment [*Google Spain*] and the present matter in that, that case involved the question of whether the relevant processing of data was covered by the protective framework, which was introduced by Directive 95/46 […]. It was, in my view, in light of that, the Court gave a broad interpretation of the second condition of this Directive's Article 4 subsection 1, point a), in order to avoid that such processing would escape the obligations and guarantees laid down by this Directive.
>
> In the present case, it must instead be determined to which of several national laws' implementation of this Directive the operations concerning processing of data that the contested terms relate to, shall be subjected.[23]

This represents a valuable first step towards reining in the scope of Article 4 (1)(a), and I will have reason to discuss it in more detail in the below.[24]

In the end, Advocate General Saugmandsgaard Øe concluded that:

> [A]n operation concerning the processing of personal data can only be subject to the legislation of a single Member State. That Member State is that in which the controller has an establishment or a body – in the sense that it there exercises a real and actual activity via a

[21] Opinion by Advocate General Henrik Saugmandsgaard Øe in *Verein für Konsumenteninformation*, Court of Justice of the European Union, C-191/15, June 2, 2016, para 119.
[22] *Ibid*., para 120.
[23] *Ibid*., paras 124-125 (author's translation of Danish original: "Bortset fra andre forskelle med hensyn til de faktiske omstændigheder, adskiller den sag, der gav anledning til nævnte dom, sig fra den foreliggende sag ved, at den drejede sig om at tage stilling til spørgsmålet, om den omhandlede behandling af oplysninger var omfattet af den beskyttelsesramme, som var indført ved direktiv 95/46 […]. Det var efter min opfattelse i lyset heraf, at Domstolen anlagde en vid fortolkning af den anden betingelse i dette direktivs artikel 4, stk. 1, litra a), for at undgå, at en sådan behandling skulle unddrages de forpligtelser og garantier, der er fastsat i dette direktiv.
I det foreliggende tilfælde skal det derimod afgøres, hvilken af flere nationale lovgivninger til gennemførelse af dette direktiv, som de operationer vedrørende behandling af oplysninger, som de anfægtede vilkår omhandler, skal være underlagt." English version not available at time of writing).
[24] One could of course suggest that the Court in Google Spain also could have relied on Article 4(1)(c) if it would have concluded that Google Inc was beyond the scope of Article 4(1)(a). However, reaching such a conclusion is associated with its own distinct difficulties.

> permanent structure – in that the relevant operation takes place as part of that establishment's or body's activities. It is for the national court to make such an assessment.[25]

6. What we will learn from the *Facebook Fanpages* case

The background to the dispute between Wirtschaftsakademie Schleswig-Holstein GmbH (joined by Facebook Ireland Ltd) and the Data Protection Authority of Schleswig-Holstein is complex. Wirtschaftsakademie Schleswig-Holstein GmbH – an educational institution in Schleswig-Holstein (Germany) – uses Facebook's "Fanpages" to advertise its programs. Where a person visits the Wirtschaftsakademie Fanpage, Facebook places a cookie on the user's computer via which it collects and processes the user's personal data. This collection and processing, it is alleged, occurs with neither Facebook, nor Wirtschaftsakademie Schleswig-Holstein GmbH, having sought the user's consent for the collection and processing.

On 3 November 2011, the *Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein* (the Data Protection Authority of Schleswig-Holstein) ordered Wirtschaftsakademie Schleswig-Holstein GmbH to deactivate its Facebook Fanpage, threatening that failure to comply would result in a penalty being imposed. The Wirtschaftsakademie appealed the decision, and in the Administrative Court, Facebook Ireland Ltd. was summoned as a Joined Party.

We may here pause to consider the implications of the Data Protection Authority of Schleswig-Holstein's decision. Just consider how many businesses, organisations, and indeed, government agencies have a Facebook presence. Does the Data Protection Authority of Schleswig-Holstein's decision mean that they all will be required to abandon this form of outreach? The fact that the stakes are high cannot be doubted.

At any rate, the matter progressed up the court hierarchy, and the proceedings are now suspended pending a decision by the CJEU. The questions referred to the CJEU will clarify several matters, including how the concepts of 'controller' and 'processor' apply in a scenario such as that involved in the case. For our purposes here, however, focus will be placed on the questions referred to the CJEU that relate to the operation of Article 4(1). They are as follows:

> **Question 3**
> Is the supervisory authority of a Member State (in this case: Germany) under Article 4, Article 28 (6) of Directive 95/46 in cases where a parent company established outside the

[25] Opinion by Advocate General Henrik Saugmandsgaard Øe in *Verein für Konsumenteninformation*, Court of Justice of the European Union, C-191/15, June 2, 2016, para 129 (authors translation of Danish original: "[E]n operation vedrørende behandling af personoplysninger kun kan være underlagt lovgivningen i én medlemsstat. Denne medlemsstat er den, i hvilken den registeransvarlige råder over en virksomhed eller et organ – i den forstand, at denne dér udøver en reel og faktisk aktivitet via en permanent struktur – idet den pågældende operation finder sted som et led i denne virksomheds eller dette organs aktiviteter. Det tilkommer den nationale ret at foretage en sådan bedømmelse." English version not available at time of writing).

> European Union has legally independent establishments (subsidiaries) in several Member States authorized to exercise the competences under Article 28 (3) of Directive 95/46 against the establishment located within its territory even if this establishment is solely responsible for support of the sale of advertising and other marketing operations towards residents of this Member State, while – according to the inter-company distribution of tasks - an independent establishment (subsidiary) located in another Member State (in this case: Ireland) is the sole controller for the collection and processing of personal data throughout the entire territory of the European Union and thus also in the other Member State (in this case: Germany), if the decision on the data processing is actually taken by the parent company?
>
> **Question 4**
> Is Article 4 (1) (a) and Article 28 (3) of Directive 95/46 to be interpreted as meaning that in cases, in which the controller has one subsidiary that is registered in a member state (in this case: Ireland) and another legally independent subsidiary, that is registered in another member state (in this case: Germany) and that is inter alia responsible for selling advertising space and whose activities address the residents of this state, the supervisory authority that is responsible in this member state (in this case: Germany) may impose measures to enforce data protection law also against the second subsidiary, which is according to the intercompany assignment of tasks and responsibilities no controller under data protection law (in this case: the subsidiary in Germany), or may only the supervisory authority of the member state impose measures in which the subsidiary, which is the controller, is established (in this case: Ireland)?
>
> **Question 5**
> Is Article 4 (1) (a) and Article 28 (3) and (6) of Directive 95/46 to be interpreted as meaning that the supervisory authority of a member state (in this case: Germany), that exercises its powers in accordance with Article 28 (3) of Directive 95/46 vis-à-vis a natural or legal person operating in its territory for not choosing carefully a third party involved in the data processing (in this case: Facebook) on the basis that this third party violates data protection law, bound by the data protection assessment of the supervisory authority of the other member state in which the controlling third party is established (in this case: Ireland), in the sense that it must not make an inconsistent assessment; or may the acting supervisory authority (in this case: Germany) independently examine the legality of the data-processing of the third party, that is established in another member state (in this case: Ireland), as a preliminary question for its intervention in this case?
>
> **Question 6**
> Provided that the supervisory authority (in this case: Germany) has the right to examine independently: Is Article 28 (6) (2) of Directive 95/46 to be interpreted as meaning that that authority may exercise the effective powers of intervention conferred upon it in accordance with Article 28 (3) of Directive 95/46 against a natural or legal person established in the territory of that authority on the basis of a joint responsibility of that natural or legal person for privacy breaches of a third party that is established in another member state, only after requesting the supervisory authority of this other member state to exercise its powers of intervention (in this case: Ireland)?

In other words, the answer to question three will tell us whether the *Google Spain* conclusion outlined above holds also where, as is the case for Facebook, there is a dedicated entity that, at least under the inter-company distribution of tasks, is responsible for the collection and processing of personal data EU-wide. The answer to question four will tell us

whether, in this case, the German DPA may impose measures to enforce data protection law or whether that privilege is exclusive to the Irish DPA. The answer to question five will tell us the extent to which, if any at all, the Irish DPA's assessments of Facebook's activities restrains other European DPAs wishing to independently examine the legality of Facebook's data processing. Finally, the answer to question six is probably of somewhat less general applicability. It will tell us whether a DPA that finds a natural or legal person established in the territory of that authority is joint responsibile with Facebook Ireland for the latter's data processing, needs to primarily turn to the Irish DPA before exercising its own powers of intervention.

Questions three and four clearly connect with aspects of the CJEU's conclusions in the *Google Spain* case, while questions five and six equally clearly connect with aspects of the CJEU's conclusions in the *Weltimmo* case. Consequently, this matter has the potential to clarify important aspects of both those decisions. At the same time, Advocate General Saugmandsgaard Øe's Opinion in the *Verein für Konsumenteninformation* case is of obvious relevance for several of these questions.

6.1 Ensuring the applicability of Union law

It may be tempting to rush to the conclusion that this matter – at least in relation to questions three and four – has already been determined through the CJEU's decision in *Google Spain*. However, here we have reason to be careful and must first meticulously scrutinise what the Court actually said in *Google Spain*.

First of all, the *Google Spain* case is limited to search engines. While the Court most likely will see it as applicable also in the context of other online activities, such as perhaps the social media activity of Facebook, the possibility of the Court viewing the technical differences as being of relevance cannot be entirely excluded. Therefore, it would be a mistake to simply assume that the Court's reasoning in relation to search engines is not specific to search engines. After all, the Article 29 Working Party has emphasised that the role of generalist search engines is different to e.g. search tools of websites of newspapers with the consequence that what was said in *Google Spain* about search engines does not necessarily apply to the latter.[26] And if not all types of search engines are covered by the *Google Spain* decision, it may not necessarily apply beyond search engines either.[27]

More importantly, the *Google Spain* case related to the relationship between a non-EU parent company and one EU subsidiary. The same can be said about the *Facebook Fanpages* case, but with the important addition that we need to take account of a third entity – Facebook Ireland which is tasked to be the sole controller for the collection and processing

[26] 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 http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf, at 8.

[27] See, however, the view expressed in Article 29 Working Group, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* (Working Paper 179 update, adopted on 16 December 2015), at 5.

of personal data throughout the entire territory of the European Union. In other words, the corporate structure in question is significantly different.

The reason this is so important is found in the very motivation for the CJEU's broad reading of Article 4 in recent cases. The following statements found in paras 53, 54 and 58 of *Google Spain* are particularly telling (emphasis added):

> **Para 53**
> Furthermore, in the light of the objective of Directive 95/46 of *ensuring effective and complete protection of the fundamental rights and freedoms of natural persons*, and in particular their right to privacy, with respect to the processing of personal data, those words ['in the context of the activities' of the establishment] cannot be interpreted restrictively[.][28]
>
> **Para 54**
> It is to be noted in this context that it is clear in particular from recitals 18 to 20 in the preamble to Directive 95/46 and Article 4 thereof that the European Union legislature sought to *prevent individuals from being deprived of the protection guaranteed by the directive and that protection from being circumvented*, by prescribing a particularly broad territorial scope.
>
> **Para 58**
> [I]t 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[.]

All this points to the close relationship between Article 4(1) on the one hand, and Articles 7 and 8 of the EU Charter of Fundamental Rights,[29] on the other hand. Indeed, as pointed out by Kuner: "EU data protection law is based largely on fundamental rights law so that the permissibility of extraterritoriality in data protection depends largely on the extraterritorial scope of EU fundamental rights instruments."[30] In other words, it does not seem like an exaggeration to say that, to a great extent, it is a concern for the protection of the rights afforded under Articles 7 and 8 of the Charter that has driven the direction of the interpretation of the Directive's Article 4.

In *Google Spain*, the consequence of finding that Google Inc and Google Spain were separate for the purpose of Article 4(1) would arguably have been that the relevant processing was beyond the reach of the Directive.[31] At least the processing would have fallen outside Article 4(1)(a). Thus, there might have been no "effective and complete protection of the fundamental rights and freedoms of natural persons", data subjects might have been "deprived of the protection guaranteed by the directive" and the company

[28] This very point was repeated in *Weltimmo* (*Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Case C-230/14), at para. 25).
[29] Charter of Fundamental Rights of the European Union, [2010] OJ C83/2.
[30] Christopher Kuner, Extraterritoriality and regulation of international data transfers in EU data protection law International Data Privacy Law (2015)5 (4): 235-245, at 243.
[31] Although as noted above, it could be suggested that Article 4(1)(c) also could have been activated.

responsible could have been seen to "escape the obligations and guarantees laid down by Directive 95/46".

In sharp contrast, under a finding that Facebook Inc and Facebook Germany are separate for the purpose of Article 4(1)(a), Union law – including the Directive and the Charter – still applies. And while such a finding may lead to European data subjects being protected under the Irish implementation of the Directive rather than under their respective country of citizenship's implementation of that same Directive – which no doubt can be less convenient for the European data subjects – it is hardly the same as there being no protection at all. In other words, only if the CJEU concludes that the Irish implementation of the Directive is completely and utterly inadequate – an unlikely conclusion – will there be a comparable lack of "effective and complete protection of the fundamental rights and freedoms of natural persons", with data subjects being "deprived of the protection guaranteed by the directive" and the company responsible escaping "the obligations and guarantees laid down by Directive 95/46".[32] As pointed to above, this difference seems to have been of great significance in Advocate General Saugmandsgaard Øe's Opinion in *Verein für Konsumenteninformation*. And applying this reasoning to the *Facebook Fanpages* matter, it seems the threatening spell of *Google Spain* has, indeed, been broken.

6.2 The 'competitive advantage' angle

Apart from the fundamental rights issues discussed so far, Van Alsenoy and Koekkoek have pointed to another reason why the CJEU adopted a broad interpretation of Article 4 in *Google Spain*: "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 have headquarters in the EU)."[33] Whether such a perspective has affected the Court's thinking is difficult to say. However, it is undeniable that an express appetite for what – rather insincerely[34] – has been portrayed as a 'level playing field' has been a driving force behind the Regulation's attitude towards extreme extraterritoriality. For example, in a March 2014 speech, then European Commission Vice-President Reding stressed that the proposed Data Protection Regulation "is about creating a level playing-field between European and non-European businesses. About fair competition in a globalised world."[35]

[32] See also: Article 29 Working Group, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* (Working Paper 179 update, adopted on 16 December 2015), at 6.
[33] Brendan Van Alsenoy and Marieke Koekkoek, Internet and jurisdiction after Google Spain: the extraterritorial reach of the 'right to be delisted' International Data Privacy Law (2015)5 (2): 105-120, at 110.
[34] For details see e.g.: Dan Svantesson, Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation, *International Data Privacy Law* (2015) 5(4); pp. 226-234, at 230-231.
[35] Viviane Reding, 'The EU data protection Regulation: Promoting technological innovation and safeguarding citizens' rights – Intervention at the Justice Council' (Speech delivered at the Intervention at the Justice Council, Brussels, Belgium, 4 March 2014) <http://europa.eu/rapid/press-release_SPEECH-14-175_en.htm>. A similar sentiment is expressed by Jan Philipp Albrecht in Jan Philipp Albrecht, Rehgaining Control and Sovereignty in the Digital Age, in David Wright & Paul De Hert (eds.), Enforcing Privacy: Regulatory, Legal and Technological Approaches, (Springer 2016) 473-488, at 476.

This desire to protect European business may very well impact future court interpretations of Article 3. However, it should be noted that, as far as the *Facebook Fanpages* case goes, the presence of Facebook Ireland has the same impact in this context as it does in relation to the effective and complete protection of the fundamental rights – Union law is applicable in any case. Thus, there is no risk that Facebook gains a competitive advantage over EU based companies as Facebook's activity in Europe already is governed by EU law.

All this suggests that it would be naive indeed to assume that the matter raised in the *Facebook Fanpages* is a dead issue already disposed of in the CJEU's decision in *Google Spain*.

6.3 Which national version of Union law?

Turning to the *Weltimmo* decision it is obvious that the factual background of *Weltimmo* is starkly different to that of the *Facebook Fanpages* case. *Weltimmo* involved a blatant instance of a business in one Member State being set up to engage only in business in another Member State. There are no parallels to that in the *Facebook Fanpages* case.

Nevertheless, it is of course possible to give the *Weltimmo* decision a broad interpretation. Put in the context of the *Facebook Fanpages* case, it could be read to suggest that German law may be applied to Facebook Ireland in that Facebook Ireland exercises, through the stable arrangement of Facebook Germany, a real and effective activity — even a minimal one — in the context of which that processing is carried out.

Such a conclusion can, however, not be reached without stretching the concept of 'in the context of the activities of an establishment' beyond where it stands today, and the question we must ask is whether there are reasons to read *Weltimmo* this broadly. As seen in the discussion of applicability of the *Google Spain* case, such a broad interpretation cannot be justified by reference to any perceived risk that the Directive's effective operation otherwise is circumvented.

At any rate, it should also be noted that in *Weltimmo*, Advocate General Cruz Villalón devoted some time to clarifying the complex operation of Article 4(1) pointing to its dual function:

> On the one hand, it [Article 4(1)(a)] enables the application of EU law through the law of one of the Member States where data processing is carried out solely 'in the context' of the activities of an establishment situated in that Member State, even though, strictly speaking, the processing is carried out in a non-member country (as was the case in *Google Spain and Google*). On the other hand, that provision operates as a rule for determining the applicable law as between Member States (which is the question at issue in the present case). In the latter situation, Article 4(1)(a) of the directive is the provision which determines the applicable law in so far as it is a rule governing conflict *between* the laws of the different Member States.[36] (internal footnote omitted)

[36] Opinion of Advocate General Cruz Villalón in *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Case C-230/14), at para. 23,

This reasoning is supported by a statement of the EC Commission in relation to the 1992 Amended Proposal for the Directive, according to which the intention of Article 4 is to avoid two possibilities: (1) "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"[37] and (2) "that the same processing operation might be governed by the laws of more than one country".[38] Considering that it can escape no one that non-EU parties caught by Article 4 remain bound by the laws of the place they are established or operating from, the reference to 'the laws of more than one country' must be presumed to refer to the law of more than one EU country.

To this we may usefully add the guidance provided by the Preamble, which in Recital 19, states that:

> [W]hen a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils *the obligations imposed by the national law applicable to its activities*; (emphasis added)

It should here be noted that "national law" is in singular, while "activities" is in plural. This points to one law being applicable to a variety of activities carried out by an establishment such as Facebook Ireland and is, of course, in line with what has been outlined above. In addition, should further support be needed, Advocate General Saugmandsgaard Øe's Opinion in *Verein für Konsumenteninformation*, embraces the proposition that one of the purposes of Article 4 is to avoid a situation where more than one national law applies to any given operation of processing of data.[39]

These descriptions of the operation of Article 4 are useful and must necessarily guide the interpretation of Article 4(1)(a) as applied in the *Facebook Fanpages* matter. Importantly, on the Data Protection Authority of Schleswig-Holstein's reading, Article 4(1)(a) would seem to point to both Irish and German law being applicable *to the same processing operation*. On this interpretation, Ireland should apply Irish law in relation to the collection and processing occurring in the context of the Wirtschaftsakademie's Fanpage and Germany should apply German law in relation to that same collection and processing.

Reading the Article 29 Working Party's update to its Opinion concerning applicable law, one may almost think that they are endorsing this position in that they, for example, state that: "It is not at all uncommon that a company headquartered in one EU Member State and

[37] COM (92) 422 final – SYN 287, 15 October 1992, 13. Recital 20 in the preamble to the Directive gives some additional guidance as to this goal: "Whereas 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; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice."

[38] COM (92) 422 final – SYN 287, 15 October 1992, 13.

[39] Opinion by Advocate General Henrik Saugmandsgaard Øe in *Verein für Konsumenteninformation*, Court of Justice of the European Union, C-191/15, June 2, 2016, para 109. See also: Lee Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014), p. 201.

having operations in multiple EU Member States would need to comply with the laws of each of these Member States (perhaps in respect of different parts of its processing operations)."[40] and that "the [*Google Spain*] judgement [sic] also confirms that - where there is an *'inextricable link'* - according to Article 4(1)(a) of Directive 95/46/EC, there may be several national laws applicable to the activities of a controller having multiple establishments in various Member States."[41]

While one may reasonably have wished for the Article 29 Working Party to take greater care in how it expresses its influential Opinions, it must be assumed that it here refers to multiple instances of processing as opposed to single instances of processing.[42] Any other conclusion is simply untenable in light of the statement by Advocate General Cruz Villalón, the statement of the EC Commission, the quoted part of the Preamble, and the statement by Advocate General Saugmandsgaard Øe since Article 4 otherwise fails to meet the stated goal of pointing to a single law. And the only way to maintain that German law is applicable, while at the same time avoiding a clash with these clear authorities would be to say that the collection and processing in question has no connection whatsoever to Facebook Ireland which seems an unlikely conclusion.

6.4 Jurisdiction over what?

It should be emphasised that all I have discussed above relates to whether Article 4(1)(a) means that Facebook Ireland (or indeed, Facebook Inc) is subject to German law, and the Data Protection Authority of Schleswig-Holstein. Even if we conclude that this is the case, we still need to analyse exactly what powers Article 28 of the Directive afford to that DPA; and here we have several options.

For some time now, I have sought to bring attention to the need to distinguish what we can call 'investigative jurisdiction' as a separate category of jurisdiction;[43] rather than grouping it together with 'enforcement jurisdiction' as the traditional approach would have us do.[44] This distinction is of particular relevance in areas such as data privacy, and we can see the beginnings of such a distinction being expressly recognised both in the EU and beyond.[45] For example, in *Weltimmo*, the CJEU stresses that:

> [W]hen a supervisory authority receives a complaint, in accordance with Article 28(4) of Directive 95/46, that authority may exercise its investigative powers irrespective of the

[40] Article 29 Working Group, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* (Working Paper 179 update, adopted on 16 December 2015), at 6-7.
[41] *Ibid*., at 7.
[42] Such an assumption is supported by various statements made in the Article 29 Working Party's Opinions on applicable law, see e.g.: "Application of the criteria should prevent the simultaneous application of more national laws to the same processing activity." (Article 29 Working Group, *Opinion 8/2010 on Applicable Law* (Working Paper 179, adopted on 16 December 2010), at 10).
[43] Dan Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013).
[44] See, eg, S Coughlan et al, 'Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization' (2007) 6 *Canadian Journal of Law and Technology* 32, preferring the conventional three categories, including investigative jurisdiction as a component of enforcement jurisdiction.
[45] See: *Lawson v Accusearch Inc dba Abika.com* [2007] 4 FCR 314, paras [28], [42], [43].

> applicable law and before even knowing which national law is applicable to the processing in question. However, if it reaches the conclusion that the law of another Member State is applicable, it cannot impose penalties outside the territory of its own Member State.[46]

Drawing upon this, it would certainly be possible to conclude that, even where the German DPA has jurisdiction to investigate complaints against Facebook, the German DPA must primarily turn to the Irish DPA when it comes to enforcement. Such a conclusion would be rather elegant in that it would ensure that users in Germany can approach the German DPA directly with no need to turn to the Irish DPA (ensuring home-ground protection in line with other consumer areas), while at the same time Facebook can be ensured that any enforcement actions will primarily be brought in Ireland at Facebook's chosen seat in Europe.

7. Adequate protection – the real issue

At the end of the day, the real issue – what all these cases are about – is whether the relevant data subjects are afforded adequate protection of their rights and freedoms as guaranteed by Union law. In the pursuit of that goal it seems that – in light of *Google Spain* and *Weltimmo* – the CJEU will afford Article 4(1)(a) with an as wide interpretation as is needed to ensure the 'effective' and 'complete' protection of the fundamental right to privacy with respect to the processing of personal data. This may no doubt be appropriate to a degree,[47] but reasonable people may disagree on what that actually means in specific cases.

In the *Facebook Fanpages* matter, a potentially determinative factor would seem to be how comfortable the CJEU is with the idea of affording the DPA in one Member State exclusive control over a company operating throughout the EU; after all, as has been stressed above, a conclusion that Facebook Ireland rather than Facebook Germany is the proper target in this matter would still result in the German data subjects being protected by the Directive.

In *ASNEF*,[48] the CJEU made clear that:

> Directive 95/46 is intended […] to ensure that the level of protection of the rights and freedoms of individuals with regard to the processing of personal data is equivalent in all Member States. Recital 10 adds that the approximation of the national laws applicable in this area must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the EU […].

[46] *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* (Case C-230/14), at para. 57. The distinction between 'investigative jurisdiction' and 'enforcement jurisdiction' can also be seen in *Schrems* (C-362/14) in that the DPAs' investigative power, of such central importance in the Safe Harbour decision, does not fit within any of the traditional categories of jurisdiction. After all, a DPA has the jurisdiction to investigate a matter but lacks the power to declare that an adequacy finding is invalid.

[47] Dan Svantesson, Private International Law and the Internet 3rd Ed (Kluwer Law International, 2016), pp. 132-136.

[48] C-468/10.

> Accordingly, it has been held that the harmonisation of those national laws is not limited to minimal harmonisation but amounts to harmonisation which is generally complete. It is upon that view that Directive 95/46 is intended to ensure free movement of personal data while guaranteeing a high level of protection for the rights and interests of the individuals to whom such data relate […].[49]

And in the words of Advocate General Saugmandsgaard Øe's in *Verein für Konsumenteninformation*:

> The Directive is thus based on the idea that the harmonisation which it implements shall ensure a uniform level of data protection throughout the Union. Therefore, it obliges Member States to maintain mutual trust in order to prevent that a single operation must be subject to strict scrutiny under the different national laws, and thus hindering the exchange of that information.[50] (internal footnote omitted)

In other words, as the law stands, all Member States are required to provide adequate protection of the rights and freedoms guaranteed by Union law, and European data subjects, as well as those businesses that operate under EU law, are entitled to assume that such adequate protection is provided throughout the EU. Despite this harmonisation, differences still exist and the Article 29 Working Party has made the point that:

> If the company were to be only subject to the data protection law of one Member State, and not also of another, the baselines provided by the Directive would still provide a relatively high level of protection for the individuals concerned. That said, and precisely because of the current lack of full harmonisation, it does matter which Member State's law applies.[51]

The question is then whether Ireland does or does not provide adequate protection of the rights and freedoms guaranteed by Union law.[52] Here, I do not have any ambitious to address that matter. However, I want to make two crucially important points. First, if it is indeed the case that some Member States do not live up to the standard they are required to meet, that is a serious issue that goes well beyond the dispute at hand.[53] It represents a failure of the EU structure.

[49] *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* (C-468/10), *Federación de Comercio Electrónico y Marketing Directo (FECEMD)* (C-469/10) *v Administración del Estado*, paras 28-29.
[50] Opinion by Advocate General Henrik Saugmandsgaard Øe in *Verein für Konsumenteninformation*, Court of Justice of the European Union, C-191/15, June 2, 2016, para 109 (author's translation of Danish original: "Direktivet bygger således på tanken om, at den harmonisering, som det gennemfører, skal sikre et ensartet niveau for beskyttelse af oplysninger i hele Unionen. Derfor forpligter det medlemsstaterne til at udvise gensidig tillid med henblik på at hindre, at en og samme operation skal undergives en nøje undersøgelse i henhold til forskellige nationale lovgivninger, og at der derved lægges hindringer i vejen for udvekslingen af de pågældende oplysninger[.]" English version not available at time of writing).
[51] Article 29 Working Group, *Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in Google Spain* (Working Paper 179 update, adopted on 16 December 2015), at 6.
[52] For a discussion of how the Irish DPA approaches data protection, see eg: Billy Hawkes, The Irish DPA and Its Approach to Data Protection, in David Wright & Paul De Hert (eds.), Enforcing Privacy: Regulatory, Legal and Technological Approaches, (Springer 2016) 441-454.
[53] Consider e.g. the 'country-of-origin' approach adopted in Directive (EC) 2000/31 of the European Parliament and Council, 8 Jun. 2000, on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce [2000] OJ L178/1, Article 3.

Second, where we seek to overcome dysfunctional substantive law by over-extending rules regarding jurisdiction and applicable law, we are embarking down a dangerous path. The end result may well be that the underlying issues in substantive law remain unaddressed, while we are stuck with inapt rules regarding jurisdiction and applicable law that end up working poorly where they previously worked well. Put bluntly, if there is indeed a problem with how Ireland, and the Irish DPA, fulfils the human rights obligations that arise under the Charter, this needs to be addressed as such. We cannot avoid doing so by pretending that Article 4(1)(a) says something it does not actually say.

8. Looking forward (or at least ahead) to the Regulation

As already noted, while the CJEU's decisions in *Google Spain*, *Weltimmo*, *Verein für Konsumenteninformation* and the forthcoming *Facebook Fanpages* case, relate to the Directive, they will clearly also impact the interpretation of the Regulation. This is so as there are clear and obvious similarity between Article 4(1)(a) of the Directive and Article 3(1) of the Regulation. However, to fully appreciate the difference between the Directive and the Regulation on this matter, we need to look beyond those two provisions; not least since the Regulation specifically adopts the 'one-stop-shop' idea. Under this structure '[t]he DPA of the main establishment of a company in the EU will take the lead in supervising the company's compliance across the EU in accordance with the cooperation procedure.'[54] Importantly:

> [T]he criterion for determining where a company has its 'main establishment' will be the location of the company's central administration in the EU (Article 4 (13)). The 'central administration' of a controller relates to the 'effective and real exercise of management activities' that determine the main decisions regarding the purposes and means of processing through 'stable arrangements.'[55]

While this change may not necessarily alter the meaning of 'establishment', it has an obvious practical impact on how matters of establishment will be approached.

9. Concluding remarks

The above ought to have showcased that the concept of processing of personal data in the context of the activities of an establishment has undergone a significant journey over the past years; a journey that arguably has expanded the concept beyond what is likely to have been its original meaning. Further, it has been made clear that that journey is by no means over – if anything, it is just gathering pace.

It will be highly interesting to see how the CJEU tackles the *Verein für Konsumenteninformation* matter and the *Facebook Fanpages* matter. Will it follow the line

[54] C. Burton et al., 'The Final European Union General Data Protection Regulation', (2016), https://www.wsgr.com/publications/pdfsearch/bloombergbna-0116.pdf, at p. 11.
[55] *Ibid*.

of *Google Spain*? Or is the significant difference created through the presence of Amazon EU and Facebook Ireland respectively such that the *Google Spain* decision does not guide these cases? It is impossible to escape the thought that Facebook's likelihood of success would have been greater in the absence of the *Google Spain* case. Yet as outlined above, and as illustrated in Advocate General Saugmandsgaard Øe's Opinion in *Verein für Konsumenteninformation*, the *Google Spain* case does not necessarily stand in the way of the CJEU ruling in Facebook's favour. Indeed, the CJEU can do so without at all departing from the line of the *Google Spain* decision.

This highlights an interesting concern in the law making practices of courts.[56] If it is acknowledged that the outcome in the *Google Spain* case is likely to have been the same even if the Court had first dealt with the *Facebook Fanpages* matter and ruled in Facebook's favour, and yet it is also acknowledged that the outcome in the *Google Spain* case is likely to amount to an obstacle for Facebook in the *Facebook Fanpages* matter, then the unavoidable conclusion is that the order in which the Court deals with cases influences how it deals with cases – a most unsettling thought for any friend of proper functioning of the rule of law.

Indeed, it is impossible to look at present developments within EU data privacy law without the mind drifting to Fuller's work on what is required of 'good' law.[57] As is well-known, Fuller outlined eight 'distinct routes to disaster' in law making:

> The first and most obvious lies in a failure to achieve rules at all, so that every issue must be decided on an ad hoc basis. The other routes are: (2) a failure to publicize, or at least to make available to the affected party, the rules he is expected to observe; (3) the abuse of retroactive legislation, which not only cannot itself guide action, but undercuts the integrity of rules prospective in effect, since it puts them under the threat of retrospective change; (4) a failure to make rules understandable; (5) the enactment of contradictory rules or (6) rules that require conduct beyond the powers of the affected party; (7) introducing such frequent changes in the rules that the subject cannot orient his action by them; and finally, (8) a failure of congruence between the rules as announced and their actual administration.[58]

[56] I acknowledge that the claim that courts make law remains controversial in traditionalist thinking. However, as stated by Lord Reid: "There was a time when it was thought almost indecent to suggest that judges make law—they only declare it. Those with a taste for fairy tales seem to have thought that in some Aladdin's cave there is hidden the Common Law in all its splendour and that on a judge's appointment there descends on him knowledge of the magic words Open Sesame." Reid, L. 1972. The Judge as Lawmaker. Journal of the Society of Public Teachers of Law 12: 22–9, at 22. See further: Dan Svantesson, What is 'Law', if 'the Law' is Not Something That 'Is'? A Modest Contribution to a Major Question, Ratio Juris (September 2013) Vol. 26 No. 3; pp. 456-485.

[57] As was reflected in the 2014 Symposium on EU Data Protection Reform of this journal ((2014) 4(4)), I am of course not alone about being concerned about the direction of European data privacy law; see e.g. the contributions to that issue by: Radim Polcak, Getting European data protection off the ground, International Data Privacy Law (2014)4 (4): 282-289, Peter Blume, The myths pertaining to the proposed General Data Protection Regulation International Data Privacy Law (2014)4 (4): 269-273, and Bert-Jaap Koops, The trouble with European data protection law International Data Privacy Law (2014)4 (4): 250-261.

[58] Lon L Fuller, *The Morality of Law* (Yale University Press, 2nd ed, 1969) 39. Kuner discusses Fuller's work applied to the data privacy area in more detail in: Christopher Kuner, The "Internal Morality" of European Data Protection Law, 6 (November 24, 2008) available at http://ssrn.com/abstract=1443797 or http://dx.doi.org/10.2139/ssrn.1443797.

Several of these 'distinct routes to disaster' seem at risk of being present in the context of EU data privacy law generally, and in the context of Article 4 in particular. However, the stand-out here, not least in the context of Internet conduct, is of course the fourth – a failure to make rules understandable. As astutely noted by Advocate General Jääskinen:

> [T]he Directive and Article 4 thereof were adopted before the large-scale provision of on-line services on the internet started. Moreover, in this respect, its wording is not consistent and is incomplete. It is no wonder that data protection experts have had considerable difficulties in interpreting it in relation to the internet.[59] (internal footnote omitted)

I am afraid that it is impossible to avoid the conclusion that the current broad reading of Article 4 of the Directive could not reasonably be predicted and understood from the text of the Directive, so as to allow parties to adjust their conduct in order to ensure compliance. This is a real concern.

However, this situation may also represent an opportunity. Where legislators draft unclear law, Courts have a wider discretion of interpretation. The CJEU has been able to shape the meaning of Article 4 to a great extent and has generally done a good job at doing so in *Google Spain* and *Weltimmo* as supplemented by Advocate General Saugmandsgaard Øe's valuable Opinion in *Verein für Konsumenteninformation*. With the *Facebook Fanpages* matter, the CJEU has the opportunity to take the final step in giving Article 4(1)(a) a sensible balanced meaning; abit late one may feel as the Directive turns 21, but then as the interpretation we give Article 4 will impact the meaning of the Regulation's Article 3, doing so remains of the greatest importance.

Addendum

As this article was about to get published, the CJEU handed down its judgment in *Verein für Konsumenteninformation* (C-191/15). The Court of Justice took a view similar to that of Advocate General Saugmandsgaard Øe, concluding that:

> Article 4(1)(a) of 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 must be interpreted as meaning that the processing of personal data carried out by an undertaking engaged in electronic commerce is governed by the law of the Member State to which that undertaking directs its activities, if it is shown that the undertaking carries out the data processing in question in the context of the activities of an establishment situated in that Member State. It is for the national court to ascertain whether that is the case. (para. 82)

[59] Opinion of Advocate General Jääskinen in *Google Spain SL, Google Inc v Agencia Española de Protección de Datos (AEPD)* (Case C-131/12), para 61.

The CJEU's judgment lacks the clarity of Advocate General Saugmandsgaard Øe's Opinion. Nevertheless, one thing is particularly telling; that the Court does not refer to the *Google Spain* anywhere in its reasoning. Surely this must mean that it does not see *Google Spain* as a relevant precedent in relation to the category of intra-European cases (as opposed to international cases like *Google Spain*) that the *Verein für Konsumenteninformation* and the *Facebook Fanpages* matters fit within.

It should also be noted that, while the CJEU's decision does not expressly adopt the clear line of the Advocate General Saugmandsgaard Øe's conclusion that "[A]n operation concerning the processing of personal data can only be subject to the legislation of a single Member State.", it says nothing that opposes or contradicts this view. If it had been the case that the Court was of the view that Advocate General Saugmandsgaard Øe was entirely wrong in this regard, it would obviously have been prudent to point that out in a clear manner. This is no doubt obvious to the Court, and thus, it seems logical to read the silence on this important point as agreement with Advocate General Saugmandsgaard Øe's conclusion.