International Data Privacy Law Advance Access published December 23, 2010

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?

Lokke Moerel*

Abstract

- Discusses the key concepts of the provision for applicability of EU data protection laws to non-EU websites and provides for a uniform interpretation thereof based on the legislative history of the Directive.
- Discusses the differences in the manner in which the applicability rule is implemented in the Member States and the resulting divergent interpretations by the national Data Protection Authorities.
- Analyses the present means used by websites worldwide to collect the personal data of their visitors, like cookies, JavaScript, ad banners, and spyware.
- Evaluates whether the applicability rule should lead to application of the EU data protection rules to the processing of personal data of EU citizens by non-EU websites.

With the maturing of the internet, EU citizens increasingly visit EU and non-EU websites alike. Most websites track the 'click stream data' (the surfing behaviour) of their visitors to make an inventory of their interests and requirements. Based on this information websites tailor the content of their websites to the individual likings of their visitors and present them with targeted advertising. Click stream data is collected by means of various techniques like 'cookies' or the online use of JavaScript, ad banners, and spyware.[1] The use of these techniques has led to an unprecedented processing of EU personal data outside the EU. This form of behavioural marketing obviously leads to concerns about the protection of privacy of EU citizens[2] and a wish to extend the protection afforded by the Data Protection Directive to include such foreign processing of EU originating data.

I. Introduction: the applicability regime of the Data Protection Directive

It is clear that the Data Protection Directive[3] dates from the time the internet was not yet widely used. The applicability regime of the Data Protection Directive was not devised with the vast increase in cross-border flows of personal data in mind which came with the maturing of the internet. Although the Data Protection Directive has a 'long arm' reach, the connecting factor for applying the Data Protection Directive is based on the territoriality principle and limited to situations where foreign controllers use processing 'equipment' located within the EU. As non-EU websites do not use such processing 'equipment' in the EU, the Data Protection Directive does not seem to apply to the processing of data by foreign websites. Despite this, the Article 29 Working Party took the

* Partner ICT at De Brauw Blackstone Westbroek, Amsterdam, the Netherlands and researcher at TILT (Tilburg Institute for Law, Technology and Society), Tilburg, the Netherlands. This article is based on a paper presented at the 2009 ESIL-ASIL Research Forum 'Changing Futures? Science and International Law', held in Helsinki, Finland, October 2009.

1 See for definitions sections VI.3 and VII.2 of this article.

2 European Commissioner Reding has warned in a speech that the European Commission would not shy away from taking action if behavioural targeting interfered with European citizens' privacy rights, see <www.ec.europa.eu>.

3 Directive 95/46/EC of the European Parliament and 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 L281/31 ('Data Protection Directive').

position that EU data protection laws also apply if non-EU websites process the personal data of EU citizens if these data are collected by means of so-called 'cookies' or the use of JavaScript, ad banners, and spyware. As almost all websites use one or more of these tools, which results in the applicability of the Data Protection Directive to websites worldwide. Though fully understandable or even commendable from a protection point of view, this expansive interpretation seems contrary to the legislative history of the Data Protection Directive and further leads to the application of EU data protection laws whenever the data of an EU citizen are processed. Most commentators consider this an unacceptable form of 'regulatory overreaching' as there is no hope in enforcing EU data protection laws on such a scale. In any event the lack of guidance in the Data Protection Directive on the key concept of what constitutes 'equipment' has confused many national legislators and led to an unacceptable variation in national implementation provisions.[4] As a consequence, the national Data Protection Authorities are largely left to their own devices as to when to apply their data protection law, and in practice do so in a divergent manner.[5] The Data Protection Directive thus fails to meet its broader legal purpose to work as a single market measure.[6] In this paper an attempt is made to provide a uniform interpretation of the applicability rule based on the legislative history of the Data Protection Directive and suggestions are made for amendment of the applicability provisions as a basis for further discussions.

I.1 Outline

The key provision for the applicability of the EU data protection laws to non-EU websites is Article 4(1)(c) of the Data Protection Directive. To understand the scope of this provision knowledge is also required of Article 4(1)(a) of the Directive, which is discussed in section II.1. In section III, I derive the meaning of Article 4(1)(c) based on the legislative history of the Data Protection Directive. In section IV, each of the key concepts of this provision is reviewed. Section V gives a summary of the requirements for application of Article 4(1)(c). In section VI, Article 4(1)(c) is applied to the processing of personal data by non-EU websites. Section VII discusses the deviating opinion of the Article 29 Working Party in its Working Document on Non-EU Based Websites.[7] Section VIII gives a proposal for revision of Article 4(1)(c). My conclusions are presented in section IX.

II. The applicability regime of the Data Protection Directive

Article 4(1)(a) of the Data Protection Directive contains the main default rule of the applicability regime. Both provisions (a) and (c) are based on the so-called 'territoriality principle' (whereby the connecting factor is the location of the actors) rather than the protection principle (whereby the connecting factor is the location of the persons to be protected, which places the emphasis on the actions of an actor). This is explained in more detail below.

II.1 Article 4(1)(a) Data Protection Directive

According to Article 4(1)(a) of the Data Protection Directive applies 'to the processing of personal data in the context of the activities of an establishment of the controller on the territory of the Member State'.

The territoriality principle here has a more or less 'virtual nature'. The formal place of establishment of the controller is not relevant for the applicability of the Data Protection Directive.[8] The Directive is already applicable if the data processing is carried out in the context of the activities of an establishment of a controller which is located on Community territory. The controller of the data itself may be established outside of the EU.

Article 4(1)(a) of the Data Protection Directive further applies regardless of where the actual processing takes place. The EU data protection laws apply when the data processing takes place 'in the context of the activities' of an establishment. The provision does not say that the data processing must be carried out by the establishment in a Member State. On the contrary, the European legislators meant to abstract from the location where the data processing takes place. If location were to be decisive, this would easily facilitate by-passing the national data protection laws, for

4 See for a comprehensive overview of the differences Korff, 'EC Study on Implementation of Data Protection Directive, Comparative Summary of National Laws', Cambridge, September 2002, (Study Contract ETD/2001/B5-3001/A/49).

5 See Korff for examples and further section III.1 below and n 44.

6 The legal basis for the Data Protection Directive is Article 95 (formerly 100a) of the Consolidated Version of the Treaty establishing the European Community, [2002] OJ C325 ('EC Treaty'); see further Recitals 1–9 of the Data Protection Directive.

7 Article 29 Working Party, 'Working Document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites' (WP 56, 30 May 2002), at 6.

8 See Lokke Moerel, 'Back to Basics: wanneer is de Wet bescherming Persoonsgegevens van toepassing?', 3/2008 Computerrecht at 81.

instance by relocating the servers to another jurisdiction.[9] It is therefore possible that the data processing takes place in the context of the activities of an establishment in a Member State, but that the data processing itself is carried out by a third party outside this Member State (whether in another EU Member State or outside the EU). This underlines the long-arm reach of the Data Protection Directive.

In today's context this has become a matter of course. Many multinational companies now process data centrally. For instance, a foreign parent company often also processes data of its EU group companies for central management purposes. If that processing also takes place in the context of the activities of these EU group companies (for instance, the foreign parent company operates a central HR system both for its own central management purposes, but also for HR purposes of the EU group companies), the EU data protection laws will apply to those parts of the central processing which relate to the respective employees of the EU subsidiaries. This applies also if the relevant parent company outsources the central processing to yet a third party outside the EU.

Despite abstracting from the location of the data controller and the location of the data processing, the 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). That Article 4(1)(c) is based on the territoriality principle rather than the protection principle is further reflected by the fact that the nationality of the persons whose data is processed is of no relevance. The Data Protection Directive may well apply to data of non-EU nationals if these are processed in the context of the activities of an establishment in an EU Member State.[10]

(a) Commentary by Dammann and Simitis

That the European legislators indeed had the above in mind when drafting the Directive is confirmed by the leading commentary on the Data Protection Directive of Dammann and Simitis. Simitis was one of the drafters of the Directive and is generally considered to have 'grandfathered' the Directive. As this commentary is no longer generally available, there follows an unofficial translation into English:

> The Directive adopts the place of establishment of a controller as the decisive connecting factor. With the implementation of the Directive, each member state has to extend this to all processing that takes place in the context of the activities of an establishment on its territory (1 sub a first sentence). Only on the surface of things did the Directive thus adopt a 'personal' connecting factor to the detriment of the originally favoured territoriality principle, whereby the location of the processing or the place where the data are located was decisive. The directive does not take into account the 'person involved' (his domicile or nationality), but the controller of the processing and then not the place of establishment of the parent company of the controller, but the place of establishment of an establishment of the controller in the context of which the processing activities take place. The directive herewith creates a decentralization which to a large extent results in the territoriality principle, ie what is decisive is the place of processing. As a rule this has as a result that also the persons involved can rely for maintaining their own rights on their own well-known law.'[11]

(b) Applicability of Article 4(1)(a) to non-EU websites

In case of data processing by a non-EU website it is possible that Article 4(1)(a) leads to applicability of the Data Protection Directive. This would be the case if, for instance, a US company with an establishment in an EU Member State operates a website that processes data of visitors from the relevant EU Member State. If the processing by the US company can be considered 'to be carried out in the context of the activities of the establishment', the privacy laws of the relevant EU Member State will apply. In its recent Opinion on Search Engines,[12] the Article 29 Working Party has given some guidance when processing activities by (in that case) a US search engine can be considered 'to be carried out in the context of the activities of an establishment in the EU':

> However, a further requirement is that the processing operation is carried out 'in the context of the activities' of the establishment. This means that the establishment should also play a relevant role in the particular processing operation. This is clearly the case, if:
>
> –an establishment is responsible for relations with users of the search engine in a particular jurisdiction;

9 See Recital 18 of the Data Protection Directive. This is also the position of the Article 29 Working Party, see for instance 'Working Document on non-EU Based Websites' (n 7), at fn 17.

10 The Data Protection Directive makes no reference or distinction based on theh nationality of the data subject. See Ulrich Dammann and Spiros Simitis, *EG-Datenschutzrichtlinie* (Nomos Verlagsgesellschaft 1997) at 127–28; Article 29 Working Party, 'Working Document on non-EU Based Websites' (n 7), at 7.

11 Damman and Simitis (n 10), at 127–8.

12 See Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' (WP 148, 4 April 2008), at 10.

–a search engine provider establishes an office in a Member State (EEA) that is involved in the selling of targeted advertisements to the inhabitants of that state;

–the establishment of a search engine provider complies with court orders and/or law enforcement requests by the competent authorities of a Member State with regard to user data.'

Obviously, similar factors will apply in case a US company with an establishment in the EU (instead of a search engine) operates a website which processes data of visitors from the EU. Such processing of data will be considered to be carried out (also) in the context of this EU establishment if:

- the establishment is responsible for relations with the users in the relevant EU country (if for instance the website sells products or services and the establishment is involved in delivery and (after) sales services);
- the website is promoted by the establishment by means of local targeted advertisements to the inhabitants of that state.

If the relevant establishment has no involvement with the relevant customers in respect of the delivery and (after) sales services, Article 4(1)(a) will not apply.

Because the above may be somewhat abstract, a case is given to illustrate the grey areas here. For the sake of simplicity (and because I am Dutch), I use a Dutch example.

Case I: US website for product support

A US parent company offers product support through a US website, offering customers of its worldwide group companies an opportunity to submit support issues through a US based website about products brought onto the market by those worldwide group companies. The Dutch establishment has access to the information collected through the US website, insofar as complaints of Dutch customers are involved. The information is necessary for the Dutch establishment for purposes of repairs or replacement of returned products. The US parent company is the controller for the processing of the data that takes place in the context of the US website (it determines the purpose and means).

Is the Dutch Data Protection Act applicable? The data are processed by the US parent company '(also) in the context of the activities of the Dutch establishment', ie are used by the Dutch establishment to perform repairs and replacements. This involves support for the products that would otherwise have been provided by the Dutch establishment itself. Now given that the data are necessary for activities of the Dutch establishment, it must be concluded that the data are also processed in the context of the activities of this establishment. The US parent company is directly subject to the Dutch Data Protection Act.

What if the support data are not available in the Dutch establishment? Should the conclusion then be that these data are not processed (also) 'in the context of the Dutch establishment'?[13] The answer is: it depends. Possibly, the handling of complaints has been organized in such a way that it is not necessary to provide the Dutch establishment with these data, whereas the complaints-handling is still to such an extent linked to the products brought onto the market by the Dutch establishment that processing should indeed be deemed to take place (also) in the context of the Dutch activities. According to the criteria formulated by the Article 29 Working Party in its Opinion on Search Engines, the answer could be yes, if the Dutch establishment were to be 'responsible for the relations with the Dutch customers' and is 'involved in the targeted advertisement for the relevant service in its jurisdiction'. This is without doubt a grey area. In my view, however, the processing should in this case be seen as a separate activity. The support activity is apparently an activity that can be performed by a third party (in this case the parent) independently from the Dutch establishment.[14] In that case the processing does not take place (also) 'in the context of the activities of the Dutch establishment.' Obviously, more guidance from the Article 29 Working Party would be welcomed here.

II.2 Article 4(1)(c) of the Data Protection Directive

Article 4(1)(c) of the Data Protection Directive complements the main rule of Article 4(1)(a).[15] It underlines the long-arm approach of the Data Protection

13 In the affirmative Blok, 'Privacybescherming in alle staten', 2005/6 Computerrecht, at 299.

14 An example of this is the maintenance of washing machines. There are enough parties in the market that offer maintenance for all brands. If such a third party processes data of Dutch customers with a Miele washing machine, this processing does not take place 'partly in the context of the activities of the Dutch Miele distributor'. The services in question are fully independent. In my view the same should apply if another company belonging to the Miele group carries out this maintenance.

15 Article 4(1)(b) requires that Member States also apply the Directive to their territories outside the territory of the European Union if those are subject to their national laws by virtue of international public law. This part of Article 4 of the Directive will not be addressed in detail here.

Directive[16] where it provides that EU data protection laws also apply in the event the:

> controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said member state, unless such equipment is used only for purposes of transit through the territory of the Community'.

By connecting the applicable law to the location of the equipment used for the processing, the Data Protection Directive still applies the territoriality principle (see further section III.2 below).[17]

In order to ensure that the data subjects can effectively exercise their data protection rights against such a non-EU controller, Article 4(2) of the Data Protection Directive subsequently provides that a non-EU controller that uses equipment on Community territory must designate a representative established on the territory of the relevant Member State.

For the interpretation of Article 4(1)(c) the legislative history of this provision is relevant.

III. The legislative history of Article 4(1)(c)

The Data Protection Directive had two draft versions:

- the Original Proposal;[18] and
- the Amended Proposal,[19] published together with an Explanatory Memorandum of the European Commission.[20]

The final text of the Data Protection Directive was adopted in 1995.

The provision of Article 4(1)(c) of the Data Protection Directive was not included in the Original Proposal. In the Original Proposal the connecting factor for choosing the applicable national law was the 'location of the data file'.[21] In order to avoid circumvention of the applicability of the EU privacy laws, the Original Proposal further provided that 'a transfer of a data file by a controller in the EU to a non-member country was not to prevent protection of the EU privacy laws'. No provision was, however, made for a possible circumvention of the EU privacy laws if the controller itself were to relocate outside the EU (ie were to have no establishment within the EU). When this gap in protection was detected, the Amended Proposal added the text of Article 4(1)(c) to the main default rule as a second ground for applicability of the Data Protection Directive.[22] This provision (and related Recital) remained unchanged in the final Data Protection Directive.

This with the exception that the word 'means' in the English version of the Amended Proposal was replaced by the word 'equipment' in Article 4 of the final Directive (note that the word 'means' was also used in recital 20 of the English version of the final Directive but remained unchanged).

The Explanatory Memorandum[23] of the Amended Proposal confirms that the main purpose of the European Commission for the Amended Proposal was (unofficial translation from Dutch):

> to avoid the possibility 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.

This rationale is expressed in Recital 12 (second sentence):

> Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out by a person who is established in a Member State should be governed by the law of that State; whereas, the fact that processing is carried out by a person

16 See also Recital 20 of the Data Protection Directive.

17 Dammann and Simitis (n 10), at 129.

18 Proposal for a Council Directive concerning the protection of individuals in relation to the processing of personal data, COM (1990) 314–12, 1990/0287/COD (the 'Original Proposal').

19 Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data (92/C 311/04), [1992] OJ C/1992/311/30) (the 'Amended Proposal').

20 See COM (92) 422 final–SYN 287, 15 October 1992, p. 13 (the 'Explanatory Memorandum'). This Explanatory Memorandum is not available on the site of the European Commission. The following is based on the Dutch version.

21 Article 4(1) Original proposal:

1. Each Member State shall apply this Directive to:
   (a) all files located in its territory;
   (b) the controller of a file resident in its territory who uses from its territory a file located in a third country whose law does not provide an adequate level of protection, unless such use is only sporadic.

22 The main default rule then still deviated from the final Directive. The full text of Article 4(1) Amended Proposal was:

1. Each Member State shall apply the national provisions adopted under this Directive to all processing of personal data:
   (i) of which the controller is established in its territory or is within its jurisdiction;
   (ii) of which the controller is not established in the territory of the Community, where for the purpose of processing personal data he makes use of means, whether or not automatic, which are located in the territory of that Member State.

23 See the Explanatory Memorandum (n 20), at 13 for the rationale for amendment of Article 4(1).

established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas, in that case, 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.

III.1 'Equipment' versus 'means'

The last minute change of 'means' in the English version of the Amended Proposal into 'equipment' in the final Directive must have been made with a particular purpose in mind (otherwise, why change it?). A possible explanation could be that the term 'equipment' would appear to have a more narrow meaning than 'means', namely suggesting a physical apparatus rather than 'any possible means'.[24] Except for the Italian and Swedish versions, however, this change was not implemented in the other language versions of the final Data Protection Directive. In these language versions (still) the word used is one which would translate into 'means' in English rather than 'equipment'.[25] As a consequence, most national implementation laws use a term that would be a translation of 'means', which has resulted in a very wide interpretation indeed by the relevant EU DPAs.[26]

For interpretation purposes the question is which of the language versions takes precedence (if any).The European Court of Justice (ECJ) has ruled that all language versions of a directive are equally authentic and that interpretation of European law requires comparison of all language versions.[27] Although in certain cases the ECJ gave precedence to the wording used in the majority of the language versions of a directive or a specific language version,[28] it appears that the Court places more emphasis on systematic interpretation of the instrument in question together with its aims and purposes than in accordance with specific language versions of the Directive:

> [E]very provision of Community law must be placed in its context and interpreted in the light of the Community provisions as a whole, regard being given to the objectives thereof and to its state of evolution at the date on which the provision in question is to be applied.[29]

Given the fact that the word 'equipment' is used in the English, Italian, and Swedish language versions only, the above rules of interpretation make it unlikely that the (arguably more narrow) word 'equipment' will prevail.[30] It is more likely that both of the terms 'equipment' and 'means' will be interpreted by the ECJ in accordance with the purpose and meaning of the Data Protection Directive as discussed above. See section IV.3 for a detailed discussion of 'equipment' and 'means'.

III.2 Commentary by Dammann and Simitis

Dammann and Simitis also emphasize that Article 4 (1)(c) in particular intends to prevent a controller that has its activities within the EU from circumventing the protection afforded by the Data Protection Directive by relocating its place of establishment outside the EU.[31] They further confirm that by connecting the applicable law to the location of the equipment used for the processing, the Data Protection Directive explicitly falls back on the territoriality principle.[32]

24 See Korff (n 4), at 48, who indicates that most examples given are the use of a telephone to collect data, the sending of paper forms to data subjects in the EU, etc.

25 The French version, for example, uses 'moyens', the Spanish 'medios', in Italian the term 'mezzi' is used and in Portuguese 'meios'. The Dutch version uses 'middelen'. Only Ireland, Sweden, Denmark and the UK use the term 'equipment' or a comparable term.

26 See Korff (n 4), at 48–51, finding that many national DPAs take 'means' to have a very broad meaning indeed, covering all thinkable means as collection of data by telephone, access of a non-EU website by means of a PC or terminal based in the EU or the sending of paper forms by a non-EU controller to EU nationals. If such a broad interpretation is given, 'in effect, all processing involves means'. In this interpretation 'equipment' or 'means' is in fact meaningless and could as well have been deleted from Article 4(1)(c). This may explain why some national implementation provisions do not contain any reference to 'equipment' or 'means'. Examples where no reference is made to these terms are the laws of Germany and Austria, which apply to all processing in Germany (Federal Data Protection Act of 15 November 2006, section 1 sub 5) and Austria (Federal Act Concerning the Protection of Personal Data, section 3 sub 1), irrespective of the presence or use of specific types of means or equipment. Danish law (The Act on Processing of Personal Data, article 4 sub 3) did implement Article 4(1)(c) but added a second provision which extends the applicability of the law to all situations where data are collected within Denmark for the purposes of processing in a third country, regardless of the means used.

27 'To begin with, it must be borne in mind that Community legislation is drafted in several languages and that the different language versions are all equally authentic. An interpretation of a provision of Community law thus involves a comparison of the different language versions', Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415.

28 Case C-64/95 *Konservenfabrik Lubella Friedrich Büker GmbH & Co. KG v Hauptzollamt Cottbuss* [1996] ECR, I-05105. In this case, most language versions of Commission Regulation 1932/93 establishing protective measures regarding the import of sour cherries referred to 'sour cherries', whereas the German version of this regulation mistakenly referred to 'sweet cherries'. However, the Court has also held in another case that under certain circumstances a single language version can be given preference to the majority of language versions, Case 76/77, *Auditeur du travail v Bernard Dufour, SA Creyf's Interim and SA Creyf's Industrial* [1977] ECR 02485.

29 Case 283/81 *CILFIT v Ministery of Health* [1982] ECR 03415, para 20.

30 Ibid.

31 Dammann and Simitis (n 10), at 129.

32 Ibid., at 129.

Here follows an unofficial translation into English of the relevant part of the commentary):[33]

> Pursuant to paragraph 1c the Directive requires from the Member States that under certain circumstances they apply their national provisions also to the activities of a controller that is established outside the Community territory, ie in a third party state, or on the high seas or otherwise outside the territory of a sovereign state. With this provision the Directive aims to avoid in particular, that controllers that conduct their activities within the Community territory, can abscond from the harmonized data privacy laws by moving their corporate seat. The Directive requires the application of national laws in those cases in which the (external) controller, for the purposes of processing personal data, makes use of equipment, automated or otherwise, situated on the territory of the relevant Member State. Thus, the Directive reverts to the principle of territoriality.

Based on the legislative history, the rationale for applicability of Article 4(1)(c) seems to be:

(i) the territoriality requirement:
the controller must have its business activities on the Community territory (albeit not by means of an establishment) and collect data in the context thereof;

(ii) the circumvention element[34]:
Article 4(1)(c) applies only if the Data Protection Directive would have been applicable were it not that the controller does not have an establishment within the EU.

IV. Review of key concepts Article 4(1)(c)

Given the complexity of the key concepts of the provision of Article 4(1)(c), each of these concepts is reviewed below. If elements of these concepts require further guidance from the Article 29 Working Party, this is specified.

IV.1 Controller (and processor)

Article 2 of the Data Protection Directive provides that the 'controller' is 'the natural or legal person, public authority, agency or any other body, which alone or jointly with others determines the purposes and means of the processing of personal data'. From the definition it follows that it is possible to have multiple controllers for the same processing (so called co-controllers).[35]

A 'processor' is 'the natural or legal person or any other body which processes personal data on behalf of the controller'. In the context of websites it will mostly be the owner of the website who is the controller of data collected through the website.

IV.2 Controller is not 'established' on community territory

The notion of 'established' is left undefined by the Data Protection Directive save for some explanatory comments in Recital 19 of the Data Protection Directive: 'establishment on the territory of a Member State' is considered to imply 'the effective and real exercise of activity through stable arrangements' and 'the legal form of such an establishment, whether simply a branch or a subsidiary with a legal personality, is not the determining factor in this respect'. In respect of websites the Article 29 Working Party states that:

> the notion of establishment of a company providing services via an Internet website is not the place, at which the technology supporting its website is located or the place at which its website is accessible, but the place where it pursues its activity. Examples are: a direct marketing company is registered in London and develops its European wide campaigns there. The fact that it uses web servers in Berlin and Paris does not change the fact that it is established in London.[36]

The Article 29 Working Party further indicated in various opinions[37] that 'the existence of an 'establishment' has to be determined in conformity with the

33 Ibid., at 129.

34 Re the purpose of Article 4(1)(c) see also Christopher Kuner, '*European Data Protection Law: Corporate Compliance and Regulation* (2nd edn, Oxford University Press 2007), at 110: 'It is useful to recall the purpose that Article 4(1)(c) is designed to play in the framework of the General Directive. The disposition of Article 4.1.c aim at covering situations in which data subjects are deprived, by an artificial manoeuvre, of the protection afforded by the Directive and situations which fall outside the scope of any protection whatsoever, even that considering transborder data flows. A German pharmaceutical company which establishes itself in Budapest and which collects data relating to medical prescriptions from a pharmaceutical network located within a Member State, in order to target European health professionals, is evidently trying to circumvent the provisions of the Directive and Article 4.1.c should apply. Article 4(1)(c) is thus a protective provision designed to prevent evasion by data controllers of their legal responsibilities through relocation of their establishments outside the EU, while using technical means located in the EU to process data in a way that would activate their legal obligations if they were established in the EU.'

35 The concept of co-controllership is under dispute in France as the definition does not incorporate the wording 'alone or jointly with others'. See also ibid., at 70.

36 Ibid. at 70.

37 See Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' (n 12), at 10.

case law of the ECJ.'[38] The ECJ[39] considers an essential factor for the concept of branch or agency 'the fact of being subject to the direction and control of the parent body'. Further conditions that have to be met according to the ECJ[40] are:

> the concept of branch, agency or other establishment implies a place of business which has the appearance of permanency, such as the extension of a parent body, has a management and is materially equipped to negotiate business with third parties so that the latter, although knowing that there will if necessary be a legal link with the parent body, the head office of which is abroad, do not have to deal directly with such parent body but may transact business at the place of business constituting the extension.

It seems that the above conditions can equally apply to determine whether certain business activities of a parent entity qualify as an 'establishment' under the Data Protection Directive. Based on the above criteria the conclusion is that all subsidiaries and most branch offices will qualify as establishments. The interesting question in the data protection context is whether a third party (ie not a subsidiary) that processes personal data on behalf of a controller could qualify as an 'establishment' of such controller. An obvious example would be the case where a non-EU website is hosted by a service provider in the EU. Relevant here is specific case law of the ECJ in respect of the circumstances under which an 'independent agent' may qualify as an establishment. According to the ECJ this depends on the degree of independence of such a third party (whether the external perception is that he is under the 'direction and control' of the parent body). If the third party agent is basically free to organize his own work and free to represent competing companies (he carries out his own decisions), such a third party does not qualify as an establishment.[41] Based on this case law some authors conclude that under very special circumstances only external specialists and service providers would qualify as someone else's establishment.[42] An example could be a far reaching form of BPO outsourcing whereby the employees of the relevant service provider are dedicated to the services and under the direction and control of the data controller. However, as a rule independent outsourcing service providers do not seem to qualify as an 'establishment' of the controller. Given the grey area here, it would obviously be welcomed if the Article 29 Working Party would elaborate under which circumstances a third party agent could qualify as an 'establishment' of a controller (if any).

Protection gap

When applying the applicability rules of Article 4(1)(a) and 4(1)(c) a gap in protection is created.[43] The cause for this is that the concepts used in these provisions are insufficiently aligned. Article 4(1)(c) provides for applicability of the Directive in situations where the controller is *not* established within the EU. However, Article 4(1)(a) does not apply in the reverse situation (that the controller is established within the EU) but applies only if the processing 'is carried out *in the context of the activities* of an establishment of the controller'. Mere establishment within the EU is not sufficient; the processing of the data should be in the context of the activities of the relevant EU establishment. Therefore in theory a controller established outside EU territory and using equipment on EU territory could avoid European privacy laws by creating an establishment within the EU. If, for example, the processing takes place only in the context of the activities of the controller in the United States (and not of the establishment in the EU), the Directive does not apply on the grounds of Article 4 (1)(a). If the US controller subsequently makes use of equipment on EU territory, the Directive would not apply either, since the controller does have an establishment on EU territory. This outcome is clearly contradictory to the intention of the drafters to avoid the evasion of the Directive's regime. Some DPAs[44] apply

38 The Article 29 Working Party seems to refer to Article 43 EC Treaty on the 'freedom of establishment'. The case law it cites, however, mainly concerns situations whereby Member States violate the freedom of establishment by introducing obstacles to the setting up and managing of secondary establishments in their Member States while the primary establishment is located in another Member State and therefore seems of no relevance here. Note that the concept of 'establishment' features in many EU regulations and directives. See for instance Articles 5(5) and 13(2) of the Brussels Convention, which use the presence of an 'establishment' in a Member State as a connecting factor for jurisdiction purposes. According to the ECJ the term 'establishment' should be construed autonomously in the light of the purpose and scheme of the relevant regulation. The concept 'establishment' in the Data Protection Directive will therefore have to be construed in accordance with the purpose and scheme of the Data Protection Directive. See concerning Article 5(5) Brussels Convention: Case 33/78, *Somafar SA v Saar-Ferngas AG* [1978] ECR 02183. See in detail Foss and Bygrave, 'International Consumer Purchases through the Internet: Jurisdictional Issues pursuant to European Law', 2000 International Journal of Law and Information Technology, volume 8, at 99–138, and Oren, 'Electronic Agents and the notion of Establishment', at 8, available at <www.eclip.org>.

39 Case 139/80, *Blanckaert & Willems PVBA v Luise Trost* [1981] ECR 00819, para 9.

40 Case 33/78 *Somafar SA v Saar-Ferngas AG* [1978] ECR 02183.

41 Case 139/80 *Blanckaert & Willems PVBA v Luise Trost* [1981] ECR 00819.

42 Mankowski, in Ulrich Magnus and Peter Mankowski (eds), *Brussels I Regulation* (Sellier European Law Publishers 2007) at §§ 279 and 292–5.

43 See also Blok (n 13), at 297–304 and 301–2.

44 In particular the French and the Dutch DPAs. See Fonteijn-Bijnsdorp, 'Art. 4 Wbp revisited': enkele opmerkingen inzake de toepasselijkheid van de Wet bescherming persoonsgegevens', 6/2008 Computerrecht at 285–9.

Article 4(1)(c) despite the fact that the controller does have an establishment within the EU. They consider the branch or subsidiary to (also) qualify as 'equipment'. In its recent Opinion on Search Engines,[45] the Article 29 Working Party explicitly indicated that Article 4(1)(a) applies to the detriment of Article 4(1)(c) in case a controller does have an establishment in the context of which the data is processed.[46] Based on the purpose of the Directive (to avoid circumvention), there are strong arguments that in case the processing cannot be considered to be carried out in the context of an establishment (in which case Article 4(1)(a) does not apply) such establishment may also be discarded for the application of Article 4(1)(c) which will then apply if use is made of 'equipment' in the EU (independently of the relevant subsidiary).[47]

IV.3 Equipment

The legislative history of the Directive provides little guidance for the concept of equipment. From the Explanatory Memorandum,[48] which gives as examples 'terminals, questionnaires, etc', it can be derived that the drafters of the Directive had physical objects in mind (both automated and non-automated) which the data controller could locate in a Member State and use to collect data on EU citizens.[49] Dammann and Simitis give a comprehensive summary of the thinking at the time where they give two examples[50] where a controller does not have an establishment in the EU but is still active on EU territory and processes the data of EU citizens. The first is where the controller uses automated equipment to process, for instance, orders for goods within the EU which (by means of telecommunications equipment) are subsequently dealt with from outside the EU without such controller having an establishment within the EU. The second is where the data controller conducts business within the EU by means of travelling salesmen and collects data by means of questionnaires, etc:

> Automated equipment in terms of the Directive is for example an EDP-system which is physically located within the territory of a Member State, through which EDP-system information services are provided or through which EDP-system orders for goods can be received electronically and which EDP-system is not administered through an establishment in the relevant Member State, but through control and maintenance by means of telecommunication from outside the Community territory. If such system is merely electronically accessible via a telecommunication network in a Member State, whereas it is physically maintained in a third party State, the Directive does not apply. In such case, it is not the controller but the user that makes use of automated equipment located within the Community territory.

The Directive also requires the application of national law in case the controller established in a third party State makes use of 'non-automated' equipment situated in the relevant Member State. This applies for example when travellers instructed by the controller collect data in the context of sales or market research and process this in the form of collections of questionnaires or indexes, without the justification of an establishment. If the controller, established in the third party state, communicates with the traveller within the Community territory by means of mail or telephone, it cannot be established that he makes use of non-automated equipment.[51]

IV.4 Equipment situated on the territory of a member state

From the above quote from Dammann and Simitis it is clear that the drafters of the Directive had the physical location of physical objects on EU territory in mind.[52]

45 See Article 29 Working Party, 'Opinion 1/2008 on data protection issues related to search engines' (n 12), at 11: 'a Member State cannot apply its national law to a search engine established in the EEA, in another jurisdiction, even if the search engine makes use of equipment. In such cases, the national law of the Member State in which the search engine is established applies.'

46 See also in a different context Kuner (n 34), at 122, who indicates that 'a corporate subsidiary should not be considered to be "equipment" of the non-EU company'. He considers this might be different if the subsidiary is a branch office only. The latter does not seem correct.

47 Independently as, in case the equipment is operated by the establishment, the likely conclusion will be that the relevant processing will (also) be carried out in the context of the activities of the relevant establishment.

48 Explanatory Memorandum (n 20), at 14.

49 See Kuner (n 34), at 120, where he concludes that the use of the term 'equipment' betrays the origins of the Data Protection Directive in the pre-internet area, at which time 'the concept' 'was generally thought to refer to a computer, telecommunications network, or other physical object which the data controller could locate in a Member State and then operate remotely from an establishment outside the Community. What evidently was not contemplated at the time of drafting was the existence of a ubiquitous, seamless information network (ie the internet) which, owing to its decentralised nature, would routinely allow EU citizens to transfer back and forth to millions of computers throughout the world.'

50 Note that the examples given in the Explanatory Memorandum (terminals and questionnaires) are also used in the examples given by Dammann and Simitis.

51 Dammann and Simitis (n 10), at 129–30.

52 Kuner (n 34), at 123, comments (in respect of the question whether software can constitute equipment) that: 'it stretches to incredulity to describe a series of electrical impulses downloaded over the internet to a computer in the EU as "situated" within such country'.

IV.5 Making use of equipment

According to Dammann and Simitis, a controller can further only 'make use of' equipment when the equipment is within the actual control of the controller.[53] In this very capability to exercise control lies the legitimization of submitting the non-EU data controller to the law of an EU Member State. Normative here is the controller's ability to control the manner in which the processing takes place, not the ownership of the equipment:[54]

> One can only say that the controller 'makes use of equipment', if he is in actual control of this equipment. This provides the legitimation to subject him to the laws of a Member State. Decisive herefor is the control over the manner of processing personal data, whereas the private law ownership and the bearing of costs are not decisive.

IV.6 For purposed of transit only

If the equipment located on the territory of an EU Member State is used 'only for purposes of transit through the territory of the Community', the use by a controller outside the EU of this equipment will not lead to applicability of EU law. Dammann and Simitis comment that in the event of 'naked transit through Community territory' the Data Protection Directive assumes that the rights and freedoms of EU citizens are not 'affected' in a particular manner.[55]

V. Summary rationale Article 4(1)(c)

Based on the legislative history, the requirements for applicability of Article 4(1)(c) may be summarised as follows:

(i) the territoriality requirement: the controller must have its business activities on the Community territory (albeit not by means of an establishment) and collect data in the context thereof;

(ii) the circumvention element: Article 4(1)(c) applies only if the Data Protection Directive would have been applicable were it not that the controller does not have an establishment within the EU;

(iii) equipment must be physical objects physically located on EU territory;

(iv) in order to 'make use' of equipment the equipment must be 'under the control of the controller' (he should be able to decide the manner of processing, ownership is not relevant);

(v) the laws do not apply if the equipment is used for transit purposes only.

Whether Article 4(1)(c) applies in any given case should be decided based on these requirements.

An example of potential applicability of Article 4(1)(c) that was totally unforeseen by the drafters of the Data Protection Directive is the case where, for instance, a US based company outsources its IT to an EU outsourcing supplier. As a consequence, US data will be stored and processed on servers located in the EU (the servers qualifying as 'equipment') whereby such data processing cannot be considered merely for transit purposes. This happens more and more as companies implement so-called 'follow the sun' arrangements ensuring around the clock ICT or helpdesk support for the whole company against lowest cost (ie by making use of regular working hours of locations around the world). As a consequence, EU data protection law is applicable while the data processed concerns US data only (which falls within the EU scope because these data are exported to the EU and transferred back again to the USA). Many DPAs have indicated that insofar as the relevant data is indeed coming from outside the EU and transferred back again, enforcement of the EU data transfer rules 'will not be their priority'.[56] Applying the above requirements would not lead to applicability of Article 4(1)(c), since the controller (i) does not have business activities on EU territory; (ii) the data are not processed in the context of these business activities; and (iii) there is no circumvention of Article 4(1)(a) by using technical means located in the EU rather than

53 Kuner, ibid., at 121 (with reference to Dammann and Simitis) comments: 'In fact "make use" here should be interpreted in the sense of "determines", ie, the data controller must control how the equipment is used to process data, so that the English term "makes use2 is a misnomer. It is true that it is not necessary that the controller exercise full control over the equipment. The necessary degree of disposal is given if the controller, by determining how the equipment works, is making the relevant decisions concerning the substance of the data and the procedure of their processing.'

54 Ibid.

55 Dammann and Simitis (n 10), at 130.

56 Korff (n 4), at 50, quotes the UK Information Commissioner's Office (the UK DPA): 'It is hard to see the justification for applying the Directive to situations where a data controller is not established in any Member State but nevertheless uses equipment in a Member State for processing. If, for example, a business in the US collects personal information on US citizens in the US but processes the personal data on a server in the UK it is subject to the requirements of the Directive. This extra-territorial application of the law makes little sense, is very difficult if not impossible to enforce and is a disincentive for businesses to locate their processing operations in the EU. If a collection of personal data is controlled and used in a non-EU jurisdiction regulation should be a matter for that jurisdiction regardless of where the data are actually processed. Furthermore the Directive requires that a data controller outside the EU appoints a representative in the Member State where processing takes place. What is the purpose of this? There is no apparent basis on which the Commissioner could take action against a representative for a breach of UK law by a data controller established outside the EU.'

having these performed by an establishment within the EU. Article 4(1)(c) should therefore not apply. Explicit guidance from the Article 29 Working Party would obviously be welcomed here.

VI. Application of Article 4(1)(c) to data collection by non-EU websites

Hereafter follows an assessment of whether the telecommunications and other equipment involved with data collection by foreign websites constitutes the 'making use of equipment situated on EU territory'. There are many types of 'equipment' involved with collecting data on the users visiting a website. Next to the user's computer (see section VI.1) and (the hard- and software of) the underlying web server of the website, the entire physical connection between the user's computer and the website is involved in this collection of data (including the equipment of the access provider of both the user and the website) (see section VI.2). In many cases the content of web pages is further provided by websites or web servers of third parties and this 'content' may also play a part in the data collection. Websites may further make use of tools like cookies, JavaScript code, banners, and spyware to collect data. From the Working Document on Non-EU Based Websites it may be derived that the use of these tools may also constitute the use of equipment (see section VI.3).

VI.1 Personal computers

Users require a personal computer in order to be able to visit a website. From a technical perspective a website visit works as follows. When a user types the address of a website into the internet browser operating on his computer and presses return, the browser sends a request to the website's server for the page in question. The server sends the requested web page to the computer of the user. The web page is subsequently executed by the web browser. Most websites are written up in the language 'Hypertext Markup Language' (HTML), the 'regular' language in which web pages are written. HTML contains the possibility to request information from the user, such as name and contact details which can be sent to the web server operating the website. A regular visit to a website can therefore involve the processing of the personal data of the user (without the use of cookies or JavaScript, see section VI.3 below).

It is clear that the internet browser and the personal computer of the user play a role in the visit to the website. The question is whether this constitutes 'use' by the website 'of equipment situated within the EU' when collecting the data. Applying the rationale of Article 4(1)(c) the answer should be: no. The personal computer of a user is under the control of the user rather than of the website. The website therefore does not actively 'make use of this equipment' to collect data.[57]

VI.2 Communications network

Both users and websites require access to the internet via an internet service provider who deploys a host of equipment to provide the physical connection between the user's computer and the website.

For the same reasons as set out above in respect of the personal computers of users, the use of telecommunications equipment will not constitute 'the making use of equipment'. It is not the website but rather the user who makes use of the telecommunications network to access the website and in any event the telecommunications network is not under the control of the website. Any other interpretation would amount to Article 4(1)(c) always being applicable, as in all cases telecommunication lines are required for accessing a website.[58]

See along the same lines (in respect of communications equipment for transmission of e-mails) Recital 47 of the Data Protection Directive:

> Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the

57 See also Kuner (n 34), at 120–1: 'While the type of device (a computer) would qualify as "equipment" within the meaning of the term as the drafters of the General Directive seemed to have conceived of it (ie, as a physical object which processes the personal data of a data subject), it is also necessary under Article 4(1)(c) that the data controller outside the EU "make use" of the equipment (in this case, the data subject's computer) in order for Member State law to be applicable. In cases where an internet user in the EU is accessing a foreign website, it is the user, rather than the website, which should be considered the data controller. Moreover, even if the data controller is deemed to be located outside the EU, the mere fact that a data subject located in the EU communicates with a data controller outside it by means of a computer (for example, sends the controller an e-mail, etc) cannot under normal circumstance result in the data controller "making use" of the data subject's own computer.'

58 See also ibid., at 121–2: '[I]t is actually not the *foreign website* making use of a network in Europe, but the *European user* who does so, since it is the user who connects to the network in order to access the website, and the non-EU data controller has no control over the connection: thus, in such a case, the user, and not the network operator, should be deemed to be the data controller. More fundamentally, deeming a network to be "equipment" would be tantamount too making the entire internet subject to EU law, which would be an absurd result. This means that EU data protection law does not apply to foreign websites merely because of the fact that they can be accessed by European users.'

personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service.

VI.3 Cookies

A cookie is a small piece of text[59] (data) that is placed by a website on a user's computer. Cookies can be used for the purposes of session management (to facilitate a particular website visit, ie by tracking a shopping cart during the website visit), to facilitate future visits to the website (ie by remembering a login name or website setting (language or other preferences)) or gather information on a user's surfing activity (tracking users). Cookies may contain all kinds of data, but next to expiration date,[60] a domain name,[61] and a path,[62] it usually only contains an identification code by which the website can recognize the user and his session when the website is visited again from the same personal computer. Normally the relevant personal data, such as (past) content of shopping carts, login details, or preferences are stored on the web server (on which the website is operated). Not only is this more secure, but the information which can be stored in cookies is rather limited. Without cookies, each retrieval of a (component of a) web page would be an isolated event. Cookies are (by now) an intrinsic part of almost all websites.

From a technical perspective, cookies operate as follows. When a user types the address of a website into the internet browser operated on his computer (or a handheld device) and presses return, the browser sends a request to the website's server for the page in question. At the same time, the browser will search the user's computer for the cookie that the relevant website has placed on the user's computer. If a cookie is found, the browser will send the information contained in the cookie to the website's server. The information is then used by the website's server. If no cookie is present, the server sends the requested web page (and perhaps a cookie) to the computer of the user. The web page is executed by the web browser.

Figure 1. Screenshot of Internet Explorer cookie settings. Source: From: http://www.helpwithpcs.com/tipsandtricks/internet-explorer/disable-cookies-1.gif.

Web browsers offer the possibility for users to change the cookie settings. This can be used by users to disable cookies. Some web browsers (eg Internet Explorer) also offer the possibility to make a distinction between first and third party cookies. See Figure 1 for an example.

As cookies may in practice take many forms (varying from just containing the elementary information whereby the data itself is collected on the web server and cookies that themselves collect data), I will discuss the most elementary version as a starting point.

Case II: Cookies from non-EU websites

A US company with no establishments in the EU operates a website providing product information (but not selling products and services). The US website is not supported by local advertisements within the EU or other sales (promotion) activities within the EU. The website uses cookies to collect data from its visitors to tailor its site and banners to the preferences of the visitors. The cookie contains the elementary information of expiration date, domain name, path, and identification code only, and does not itself collect personal data (the personal data are collected on the web server in the USA).

If the website is visited by EU citizens and data on these visitors are collected from the EU, does Article 4(1)(c) apply to this processing of data?

59 Cookies are not executable and are neither software, spyware, nor viruses, although they can be used to track users. Cookies merely consist of data and allow for the exchange of information between a user's computer and the website that placed the cookie.

60 The expiration date tells the browser when to delete the cookie. By specifying an expiration date cookies are not deleted at the end of session and can be used in a next browser session. Such a cookie is called persistent. A session cookie is deleted at the end of a surfing session when the user closes the browser.

61 The domain tells the browser to which domain the cookie should be sent. If nothing is specified, it defaults to the domain of the object requested.

62 The path enables the developer to specify a directory on the web server where the cookie is active.

Applying the requirements for the application of Article 4(1)(c) to this use of cookies, the answer should be: no.

1. the territoriality principle is not adhered to:
(a) the relevant US company operating the website has no concrete business activities on EU territory (does not undertake active local advertising, has no local sales people to solicit business, etc);
(b) the EU visitors access the relevant website on their own initiative without local prompting, ie the EU citizen is not visited or contacted by whatever means within its own territory but rather itself actively seeks access to a foreign website 'outside' its own territory;
(c) the US company does not make use of 'equipment' physically situated within the EU to collect data. The cookies are used for identification purposes rather than data collection itself (which takes place within the US). The placing of the cookies did further not require actual activities of the US company within the EU.

2. there is no circumvention aspect:
the Data Protection Directive would not have been applicable were it not for the fact that the US company does not have an establishment in the EU. Even if the US company were to have had an establishment within the EU, the Data Protection Directive would not apply as the data processing cannot be considered to take place in the context of the activities of such establishment (there being no sales (promotion) activities within the EU, see section II.1(2) on the applicability of Article 4(1)(a) to non-EU websites).

3. there is no making use of equipment as there is no control:
the website owner does not have control over the cookies. The website owner can try to place them, but the user can prevent this by means of his browser settings and the user can disenable cookies at any time thereafter (see section VI.3 above).

4. there is no physical equipment that is physically situated on EU territory: cookies concern mere text and cannot qualify as a physical object. The cookies cannot qualify as equipment used for processing as the cookies are used for identification purposes rather than data collection itself (which takes place within the USA).

5. transit purposes only: as cookies do not qualify as equipment (see sections I–IV above), this exception is not relevant.

Again, as users use a personal computer to visit websites and websites use cookies to facilitate the use of websites, applying Article 4(1)(c) to any and all data processing of EU nationals whenever cookies are used would amount to applying the protection principle (relevant factor is the action: the Directive applies to the processing of data of EU users) rather than the territoriality principle (ie relevant factor is the actor, ie the location of the equipment used), which was not the choice made by the legislator.

This is also the prevailing opinion in the legal commentary.[63]

VII. The Working Party's position on cookies

The position of the Working Party is diametrically opposed to the above findings. In its Working Document on Non-EU based websites,[64] the Working party takes the position that Article 4(1)(c) does apply to data collected by means of cookies by a US website. The Working Party considers the placing of cookies on

63 See Kuner (n 34), at 125: 'The view that cookies constitute "equipment" would also in effect result in the location of the data subject (rather than the place of establishment of the data controller) always determining the applicable law, which is clearly not the principle underlying Article 4 of the General Directive'; Swire, 'Of Elephants, Mice, and Privacy: International Choice of Law and the Internet', 32 International Lawyer 991 (1998), at 1011, argues that there is no real basis for interpreting the scope of Article 4 (1)(c) to have such a wide reach (as to apply to cookies). First, if it were intended to expand EU jurisdiction law to such an extent, this would have taken place through a 'publicized or negotiated effort' instead of a provision in a specialized Directive. Second, the expansion of jurisdiction to websites around the world by means of a Directive drafted in the early 1990s, before there was any real conception of the internet and how to regulate it, does not appear to make much sense. Finally, the broad expansion of jurisdiction under the Directive raises 'traditional concerns about notice, fairness, comity and national sovereignty.' According to Kobrin, 'The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance', Working Paper Series, The Wharton School (November 2002), at 23, such an expansive interpretation of 4(1)(c) leads to a situation which he describes as 'hyper-regulation', whereby extraterritorial reach becomes the norm rather than the exception'. See along the same lines Blok (n 13), at 301 and Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation', [2000] Computer Law and Security Report 252 at 255. See also Terwangne and Louveaux, 'Data protection and online networks', 13 Computer Law & Security Report 239 (1997) who (in a publication of 1997 therefore dating well before the Article 29 Working Document on Non-EU Based Websites) consider that collection of data by a non-EU website through the use of cookies does not fall within the scope of Article 4(1)(c). They, however, are of the opinion that this results in a lack of protection of EU nationals and propose to extend the applicability of Article 4(1)(c) to situations where no use is made of equipment (ie, in case cookies are used).

64 Article 29 Working Party, 'Working Document on non-EU Based Websites' (n 7), at 11.

personal computers located within the EU as 'the making use of equipment' within the EU:

> As explained above, the user's PC can be viewed as equipment in the sense of Article 4(1) c of Directive 95/46/EC. It is located on the territory of a Member State. The controller decided to use this equipment for the purpose of processing personal data and several technical operations take place without the control of the data subject. The controller disposes over the user's equipment and this equipment is not used only for purposes of transit through Community territory.
>
> The Working Party is therefore of the opinion that the national law of the Member State where this user's personal computer is located applies to the question under what conditions his personal data may be collected by placing cookies on his hard disk.

The Working Party has taken a similar position in its earlier Working Document on Privacy on the Internet,[65] although there it did not explicitly designate the computer as the equipment. Rather, the cookie itself was designated as the 'means' through which data were collected:

> While the interpretation of the notion of 'equipment' or 'means' has given rise to debate about their extent, some examples undoubtedly fall within the scope of application of Article 4.
>
> This will be the case, for example, for a text file installed on the hard drive of a computer which will receive, store and send back information to a server situated in another country. Such text files, named cookies, are used to collect data for a third party. If the computer is situated in an EU country and the third party is located outside the EU, the latter shall apply the principles of the national legislation of that Member State to the collection of data via the means of the cookie.[66]

As a consequence, the Working Party requires that users are informed of the use of cookies when visiting a website:

> [T]he user should be informed when a cookie is intended to be received stored or sent by Internet Software. The message given to the user should specify, in clear terms, which information is intended to be stored in the cookie and for what purpose as well as the period of validity of the cookie. The user should then be given the option to accept or reject the sending or storage of a cookie as a whole and they should be given options to determine which pieces of information should be kept or removed from a cookie depending on, for example, the period of validity of the cookie, or the sending and receiving web sites.'[67]

VII.1 Review of the Working Party's underlying reasoning on cookies

The underlying reasoning of the Working Party merits a detailed discussion in order to decide whether its position on cookies is convincing or not. The short conclusion of this analysis is that the Working Party acknowledges that Article 4(1)(c) is based on the territoriality principle but subsequently makes a creative turn indeed by interpreting the territoriality principle in accordance with the protection principle (ie by concluding that the territoriality principle 'reflects a true concern to protect individuals on [their] own territory). This results *de facto* in the Working Party applying the protection principle which is contrary to the (legislative history of) the Data Protection Directive.

The Working Party starts its Working Document with a broad introduction to the question of application of the EU data protection laws to the processing of personal data by websites that are based outside the EU. It starts by indicating that this is a 'general question of international law which arises in on-line and off-line situations where one or more elements are present that concern more than one country'. According to the Working Party:

> these decisions involve a consideration of a number of factors. First and foremost, the concern of a given State is to protect the rights and interests of its citizens, residents, industry and other constituencies recognised under national law.[68]

This seems to be a reference to the *lex protectionis*, whereby the laws apply of the location of the data subject (ie of its residence or nationality). The Working Party then continues with a list of examples[69] where community law is applied on an extra-territorial basis and concludes that in these examples of Community law 'similar criteria are applied'. 'Whether it is a requirement that the relationships have a "community dimension" or "close connection" with the Community, in certain situations the European Court of Justice, the European Parliament and Council as well as the European Commission see fit to impose EU rules on non EU based entities'. In all examples given by the Working Party the extra-territorial application is based on the conventional principle of the *lex protectionis*

65 Article 29 Working Party, 'Working Document Privacy on the Internet, An integrated approach to on-line Data Protection' (WP 37, 21 November 2000), at 28.

66 Ibid.

67 Article 29 Working Party, 'Working Document on non-EU websites' (n 7), at 11.

68 Ibid., at 3.

69 Ibid, at 3–4.

(whereby the connecting factor is the location of the (legal) persons to be protected, which places the emphasis on the actions) rather than the territoriality principle (whereby the connecting factor is the location of the actors to a territory).[70]

The relevance of this summary given by the Working Party is somewhat unclear as the Data Protection Directive contains a specific provision for the applicability of the Data Protection Directive which takes priority over the general conflict rules of international private law.[71] The Working Party subsequently acknowledges this itself where it concludes the introduction with: 'Against this background, it has to be noted that the EU data protection directive contains an explicit provision on the applicable law indicating a criterion. Irrespective of whether this provision is easy to understand or to handle, it is nevertheless an advantage for the benefit of individuals and business that the data protection directive addresses this essential question'.[72]

After this catalogue of examples of EU laws based on the protection principle, it is somewhat surprising that the Working Party subsequently indicates that the explicit provision in the Data Protection Directive is one based on the physical link with a member state and that it is not the nationality of the individuals that is decisive but the location of the processing equipment. The Working Party, however, subsequently makes a full turn by then concluding that this principle 'reflects a true concern to protect individuals on [their] own territory' and that 'at international level it is recognised that states can afford such protection'. This is a creative turn indeed to transform the territoriality principle into the protection principle:

> The European Parliament and the Council decided to come back to one of the classic connection factors in international law, which is the physical link between the action and a legal system. The EU legislator chose the country of the territorial location of equipment used. The directive therefore applies when a controller is not established on Community territory, but decides to process personal data for specific purposes and makes use of equipment, automated or otherwise, situated on the territory of a Member State.
>
> The objective of this provision in 4 paragraph 1 lit. (c) of Directive 95/46/EC is that an individual should not be without protection as regards processing taking place within his country, solely because the controller is not established on Community territory. This could be simply, because the controller has, in principle, nothing to do with the Community. But it is also imaginable that controllers locate their establishment outside the EU in order to bypass the application of EU law.
>
> It is worth noting that it is not necessary for the individual to be an EU citizen or to be physically present or resident in the EU. The directive makes no distinction on the basis of nationality or location because it harmonises Member States law on fundamental rights granted to all human beings irrespective of their nationality. Thus, in the cases that will be discussed below, the individual could be a US national or a Chinese national. In terms of application of EU data protection law, this individual will be protected just as any EU citizen. It is the location of the processing equipment used that counts.
>
> The Community legislator's decision to submit processing that uses equipment located in the EU to its data protection laws thus reflects a true concern to protect individuals on its own territory. At international level it is recognised that states can afford such protection. Article XIV of the GATS allows to lay down exemptions from free trade rules in order to protect individuals with regards to their right to privacy and data protection and to enforce this law.[73]

In its subsequent interpretation of Article 4(1)(c) the Working Party interprets the provision in line with the protection principle rather than the territoriality principle (with an emphasis on the action rather than the actor) by taking the position that the sending by a non-EU based website of so-called 'cookies' to the computers[74] of internet users in the EU constitutes the use of 'equipment' in the EU. As all users require a computer to visit a website (and almost all websites use cookies) this amounts to indiscriminately applying the Data Protection Directive to all data processing of EU nationals who visit foreign websites.

From the Working Document it may also be derived that the Working Party itself is not too sure about the tenability of its position where it advocates a 'cautious approach' when applying Article 4(1)(c):[75]

> The Working Party would advocate a cautious approach to be taken in applying this rule of the data protection directive to concrete cases. Its objective is to ensure that individuals enjoy the protection of national data protection

70 Bing, 'Data protection, jurisdiction and the choice of law', Privacy Law and Policy Reporter, [1999] 65, at 7.

71 Under international private law, rules of semi-public law or special obligatory rules of private law take precedence over general rules of international private law. In this context, the Directive can be considered as containing rules of precedence as they contain mandatory rules that aim to protect a group of relatively weak legal persons, as is expressed in Recital 10 of the Directive. See Blok (n 13), at 302.

72 Article 29 Working Party, Working Document on non-EU websites (n 7), at 5.

73 Ibid., at 5.

74 The Working Party only refers to computers. By now many users access the internet by means of hand held devices (like smart phones). This will probably not change the position of the Working Party.

75 Article 29 Working Party, Working Document on Non-EU Based Websites, (n 7), at 11–12.

> laws and the supervision of data processing by national data protection authorities in those cases where it is necessary, where it makes sense and where there is a reasonable degree of enforceability having regard to the cross-border situation involved.

It may be clear that these factors are not based on the Data Protection Directive and are so vague (the Data Protection Directive applies when it 'makes sense'?) and therefore cannot constitute a valid basis for controllers to decide whether to apply the EU data protection laws.

The conclusion is that the interpretation given by the Working Party is contrary to the legislative history of Article 4(1)(c). Although the attempt of the Article 29 Working Party to provide protection to EU nationals is commendable, this result should be achieved by amendment of the applicability rule for instance by bringing this rule in line with the general rules of international private law. This should be done by the European legislators and not via the short-cut of opinions of the Article 29 Working Party.

VII. 2 JavaScript, ad banners, and spyware

A similar position (based on similar considerations) is taken by the Working Party in respect of the use of JavaScript, ad banners, and spyware. In summary, the position of the Working Party is that these 'tools' are used to collect and process data whereby use is made of the equipment of the data subject (computer, browser, hard drive). Based on the rationale of Article 4(1)(c) as applied in respect of cookies (see section VI.3 above), here the conclusion should also be that applying Article 4(1)(c) to these tools would amount to applying the protection principle (what is applicable is the law of the nationality of the user visiting the website) rather than the territoriality principle, which was not the choice made by the legislator.

Before discussing how Article 4(1)(c) may be amended, I will first briefly discuss the various national implementation provisions and the findings of the European Commission in its First Report on the implementation of the Data Protection Directive.[76]

VII.3 First Report on the Data Protection Directive

Pursuant to Article 33 of the Data Protection Directive the European Commission has to report at regular intervals on the implementation of the Data Protection Directive and, if necessary, provide suitable proposals for amendment. Based on a survey of the various national implementation provisions of Article 4(1) ('Technical Analysis')[77] the Commission concludes in its First report on the data Protection Directive that Article 4(1)(c) has not been uniformly implemented and that the substantial divergences in implementation mean that potential positive and negative conflicts of law remain between the Member States.[78]

This means that due to a lack of harmonization in the EU, controllers have to comply with deviating national laws (which create conflicts of law). Such conflicts would have been avoided if Article 4 had been uniformly implemented throughout the EU. Regarding Article 4(1)(c), the Technical Analysis mostly focuses on the use of the term 'means' versus 'equipment' (see section III.1 above).

Despite these divergences the Commission, did not recommend that Article 4(1)(c) be amended.[79] The Commission indicated that it is its 'priority to secure the correct implementation by the Member States of the existing provision' and that 'more experience with its application and more reflection is needed, taking into account technological developments, before any proposal to change Article 4(1)(c) might be made'.[80] The Commission continued that it:

> is aware that the 'use of equipment' criterion of 4(1)(c) may not be easy to operate in practice and needs further clarification. Should such clarification not be sufficient to ensure its practical application, it might in due course be necessary to propose an amendment creating a different connecting factor in order to determine the applicable law.[81]

VIII. Proposed revision of Article 4(1)(c)

When thinking about revising Article 4(1)(c), it should be taken into consideration that:

1. any connecting factor that relates to the making use of 'equipment' (even if used in a 'technology-neutral' meaning) is no longer suitable given the speed of developments whereby the 'means' used for data collecting and processing are in constant development; any connecting factor should apply irrespective of the means used.
2. the underlying principle of territoriality whereby a physical connection is required to a territory is no

76 European Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM (2003) 265 final.

77 Analysis and impact study on the implementation of Directive EC 95/46 in Member States, attached to the First Report on the Data Protection Directive ('Technical Analysis').

78 Ibid., at 7–8.

79 First Report on the Data Protection Directive (n 76), at 17.

80 Ibid.

81 Ibid.

longer suited to being applied in the current day reality.[82] The principle of territoriality can only work if it has a true 'virtual nature';

3. an unbridled expansion of applicability of EU data protection laws to processing of data on EU citizens wherever in the world should be prevented;[83] and
4. gaps in protection should be prevented (the gap in protection created by non-alignment of Articles 4(1)(a) and (c) (see section IV.2 above) should be avoided, ie these provisions should be aligned.

Without upsetting the rationale of the applicability regime of the Data Protection Directive the above factors would require that Article 4(1)(c) will be amended in such a manner that it will be a true 'virtual' reflection of the territoriality principle. This will entail:

- the elimination of any 'physical location' as a connecting factor (whether of the controller, the equipment used or the activities of the controller);
- eliminating the 'use of means' as a connecting factor;
- if the 'use of means' is no longer a connecting factor, the exception when equipment is used 'for transit purposes only' can also be eliminated;
- the unbridled application of Article 4(1)(c) to all processing through websites can be prevented by requiring that the processing takes place 'in the context of the activities of the controller on or directed at[84] the territory of the Member State';
- by using this as the connecting factor, Articles 4(1)(a) and (c) will also be aligned and gaps in the protection will be avoided.

The above, reflected in a text proposal, amounts to applying Article 4(1)(c) to situations where the

> controller is not established on Community territory but the processing of personal data takes place in the context of the activities of the controller on or directed at the territory of the Member State.

Article 4(1)(a) and (c) being thus aligned, they can then also be simply taken together by providing that the national laws apply:

> to the processing of personal data in the context of the activities of the controller on or directed at the territory of the Member State.

The Working Party can subsequently contribute by expanding on the requirements when any processing by a controller can be considered to take place 'within the context of the activities of the controller on or directed at the territory of a Member State'. This should not be problematic as this can be done along similar lines as in its Working Document on non-EU websites in respect of Article 4(1)(a), see section II.1(2) above.[85]

82 As Kobrin (n 64), at 23, states: 'Extraterritorial reach not only becomes the norm, the concept itself loses meaning as the distinction between domestic and international affairs blurs to the point where it is no longer meaningful and territoriality becomes problematic as the organizing principle underlying the international political system.' And at 28: 'Transnational integration, however, is increasingly relational rather than geographic; the new political space from which effective and legitimate governance must emerge takes the form of relational networks rather than territory, a 'space of flows' rather than a 'space of spaces'.

83 This would amount to applying the so-called 'effects doctrine', which is already in the off line world criticized as it is too open-ended, ie it leads to applying the laws of a state even if the effects are insubstantial. See Thomas Schulz, 'Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface', (2008) 19 European Journal of International Law 799, at 815. An example of an indiscriminate application of rules is the present scope of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, [2002] OJ L201/37; as revised by Directive 2009/136/EC of the European Parliament and of the Council 25 November 2009 (the 'E-Privacy Directive'). The E-Privacy Directive lacks a specific applicability regime. The prevailing view is, however, that the opt-in requirements for the use of cookies and direct e-mail apply to all interactions with internet users in the EU. This is based on Article 3(1) E-privacy Directive, which states: 'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks *in the Community*' (emphasis added). As all internet users in the EU use a public network located in the EU, the rules of the E-Privacy Directive apply to all e-mail from outside the EU to individuals in the EU as well as to all visits of EU citizens to non-EU websites. The same applies for Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, [1997] OJ L144/ 19 (the 'Distance Selling Directive'). The online contracting and information requirements of the Distance Selling Directive apply to all entities that contract for goods or services via email and internet with EU citizens, therefore also non-EU entities.

84 This element has to prevent discussions whether certain online activities of a controller should be considered to take place on the territory of a Member State. A comparable element was part of the proposed provision on applicable law and jurisdiction in the latest Madrid draft proposal for International Standards. The provision was however left out of the final version.

85 See for alternative solutions proposed in legal commentary: Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation', [2000] Computer Law and Security Report, at 262, suggests letting the protection principle prevail by amending the Data Protection Directive and making the applicable law the law of the state in which the data subject has his or her domicile. Bygrave also suggests as a possible compromise adopting a qualified version of the 'data subject domicile criterion'. This would stipulate that the data protection law of the country in which the data subject is domiciled will apply if the data controller should reasonably have expected that his processing of data on the data subject would have a potentially detrimental effect on the latter'. It is difficult to see that this would solve the problem of the EU data protection laws apply indiscriminately to all processing of data of EU nationals. The same applies to Reidenberg, Workshop 4: International issues: international data transfers, applicable law and jurisdiction (European Commission Conference on the Implementation of Directive 95/46/EC, 2002), at 3–4, who is of the opinion that 'The collection of data for processing is "doing business" within the forum where the individual is located and data protection law should require that data collectors be responsible in that forum for their activities conducted with that forum'. Kuner (n 34), at 124, suggests limiting the long reach of Article 4(1)(c) by making an analogy with the findings of the ECJ in the Lindqvist case (Case C-101/01 *Bodil Lindqvist* [2003] ECR I-12971). In that case, the ECJ found that the data transfer restrictions under Article 25 of the Directive should not become a general rule that would apply to

Relevant criteria would, for instance, be if the controller contracts with visitors from the EU, performs actual deliveries and (after) sales services in this Member State, if the website is promoted by means of local targeted advertisements to the inhabitants of that state, ie by listings with local search engines, banner advertisements on local websites, offline advertisements or product placements in shops, provision of Member State specific information (for instance the tax regime) relating to a Member State, etc.

The applicability regime of the data protection Directive is thereby also brought in line with the jurisdiction and applicable law regime for consumer contracts of Article 6 of EC Regulation 593/2008 of 17 June 2008 on the law applicable to contractual obligations ('Rome I'),[86] which provides that (in the absence of a valid choice of law) a consumer contract:

> shall be governed by the law of the country where the consumer has his habitual residence, provided that the professional [seller]:
>
> (a) pursues his commercial or professional activities in the country where the consumer has his habitual residence, or
> (b) by any means, directs such activities to that country or to several countries including that country,
>
> and the contract falls within the scope of such activities.'

Some guidance as to when there is 'directed activity' is to be found in Recital 24 to Rome I:

- it is not sufficient that an undertaking targets its activities at the Member State of the consumer's residence, or at a number of Member States including that Member State, a contract must also be concluded within the framework of its activities;
- the mere fact that an internet site is accessible is not sufficient for this provision to be applicable, although a factor will be that this internet site solicits the conclusion of distance contracts and that a contract has actually been concluded at a distance, by whatever means;
- the language or currency which a website uses does not constitute a relevant factor.

Applying these starting points to the proposed article 4(1)(c) would entail that the mere fact that a non-EU website processes personal data of visitors from the EU should not be sufficient for the Data Protection Directive to apply. Even the conclusion of an online contract alone should not be sufficient. The website owner should actively solicit those visits and sales by visitors from the EU by some activity targeted to these visitors. In most cases this will involve some local activities in a Member State (local advertisements, listings with local search engines, contacts with local distributors). In any event the text proposal for Article 4(1)(c) and the connecting factors of Rome I all have in common the need to be further expanded as these concepts all lack clarity.[87]

The acid test here is whether the consumer protection rules of Rome I would apply to, for instance, the .com website of Amazon, assuming that Amazon had no localized versions of its website, that any products bought would be sent directly by Amazon US to any consumer around the world and that the website was not supported by local advertisements or other promotions. The conclusion should be that the consumer protection rules of Rome I would not apply in those circumstances as the site would not be targeted specifically to EU citizens. In the same vein, EU national laws implementing the Data Protection Directive should not apply to any processing of personal data by Amazon of these visitors from the EU.[88]

the entire Internet without the data controller taking a positive step to actively transfer personal data outside the EU. This finding suggests that the rules of Article 4 should also not be applied to activities that could result in EU data protection law being extended to the entire Internet indiscriminately, 'unless the non-EU data controller of a website has taken some positive steps to "target" individuals in the EU.' Though commendable, this constitutes a solution which requires controllers to first apply the outdated connecting factor of 'the use of equipment situated on a member state' to subsequently apply the rule of the Lindqvist case. Terwangne and Louveaux (n 63), at 239, consider that the situation 'where a data transfer is exclusively carried out by a controller located in a third country' should also fall within the scope of Article 4(1)(c). They consider that the case when data are collected by a non-EU website through the use of cookies. They propose to extend the applicability of Article 4(1)(c) to these situations as well, ie, to situations where no use is made of equipment. Terwangne and Louveaux do not elaborate on the criteria 'when operations can be considered carried out in Europe'. They do, however, give two examples when the scope of Article 4(1)(c) needs to be extended. The examples given by Terwangne and Louveaux would already fall within the scope of Article 4(1)(c) based on the requirements identified in this paper (ie should therefore not require amendment of Article 4(1)(c)). That being said, the solution proposed by Terwangne and Louveaux is quite similar to the amendment to Article 4(1)(c) as proposed in this publication.

86 [2008] OJ L177/6. According Recital 24 of Rome I, article 6 of Rome I should be interpreted harmoniously with Article 15 EC Regulation 44/2001 of 22 December 2000 on jurisdiction and enforcement ('Brussels I Regulation'),[2001] OJ L12/1.

87 See for criticism what 'targeting' means: Uta Kohl, *Jurisdiction and the Internet: a Study of Regulatory Competence over Online Activity* (Cambridge University Press 2007) at 76–8; and Schulz (n 83), at 818.

88 By now Amazon has many localized websites around the world, including several in the EU, and visitors to amazon.com are automatically routed to those localized websites. The EU consumer and data protection rules apply to such localized websites.

IX. To conclude

At the moment there are a number of Member States that have not properly implemented the applicability rule of Article 4(1)(c) of the Data Protection Directive. Also the Article 29 Working Party uses an interpretation of this rule which seems contrary to the (legislative history of the) Data Protection Directive. Although the attempt of the Article 29 Working Party to provide protection to EU nationals is commendable, this result should be achieved by amendment of the applicability rule. This should be done by the European legislators and not via the short-cut of opinions of the Article 29 Working Party. Given the present differences in the EU implementation laws it would in any event be welcomed if the European Commission were indeed to take as its first priority to ensure the correct implementation of Article 4 of the Data Protection Directive in all Member States.[89]

doi:10.1093/idpl/ipq004

89 The European Commission has indicated that the Commission's priority is to first ensure correct implementation of Article 4 of the Data Protection Directive before effecting changes to Article 4 of the Data Protection Directive. See First Report on the Data Protection Directive (n 76), at 17. See for deviating implementations section 2.4.