EUROPEAN DATA PROTECTION SUPERVISOR

PETER HUSTINX
SUPERVISOR

Mr Alexander ALVARO
Member, European Parliament
BRU - ASP 10G146
B-1047 Brussels

Brussels, 4 February 2009
PH/RB/ktl D(2009)204 **C 2009-064**

Dear Mr. Alvaro,

This letter is to follow up on our meeting of 20 January 2009 with you and Mr. Harbour regarding the ePrivacy and Universal Services Directives.

During this meeting, you asked me to reflect on the effects on Article 6.6 (a) if the scope of the ePrivacy Directive was broadened. In particular, you asked me to consider whether any such potential effect might change my views on Article 6.6 (a).

To meet your request, I have first considered the impact on Article 6.6(a) if the overall scope of the ePrivacy were to be enlarged to apply to providers of publicly available electronic communications services in publicly accessible private networks. Additionally, I have considered how and to what extent Article 6.6(a) may be affected if the security breach provisions were to be applied to providers of electronic commerce services.

For the reasons described below, I have come to the conclusion that the enlargement of the scope of the ePrivacy Directive in either of the two aspects outlined above has no effects on Article 6.6 (a.) I do not see any reason to change my views on Article 6.6 (a), as described in my Opinion of 9 January 2009, i.e. the best outcome would be for the proposed Article 6.6 (a) to be deleted altogether.

I. SCOPE OF THE E-PRIVACY DIRECTIVE TO INCLUDE PROVIDERS OF PUBLICLY ACCESSIBLE PRIVATE NETWORKS AND ITS RELATION WITH ARTICLE 6.6 (a)

- Under the current ePrivacy Directive, telecom operators and other types of PECS[1] are entitled, within certain limits, to engage in processing of traffic data to safeguard the security of their services. This is based on Article 4.1 of the ePrivacy Directive pursuant to which such type of provider *"must take the appropriate technical and organisational measures to safeguard the security of its services."* These measures may require, among others, the processing of traffic data, for example, in the context of fighting viruses, malware, spam, etc[2]. However, traffic data can only be *retained* within the limits set by Article 6 as currently formulated.

- If the overall scope of the ePrivacy were enlarged to apply to providers of publicly available electronic communication services in publicly accessible private networks, this would mean that, in addition to telecom operators and traditional PECS, *also* providers of Internet access in Internet cafes, Wi-Fi spots available in hotels, airports, etc would benefit from Article 4.1 within certain limits, including those imposed by Article 6.

- Note that providers of publicly available electronic communication services in publicly accessible private networks *do not* include providers of electronic commerce services such as on-line retailers (**'e-commerce providers'**). Thus, the enlargement of the ePrivacy Directive to cover providers of publicly available electronic communication services in publicly accessible private networks would not automatically enable e-commerce providers to benefit from Article 4.1 of the ePrivacy Directive.

- If Article 6.6(a) as proposed by the EP were adopted, then, in addition to the two types of actors described above (PECS *and* providers of publicly available electronic communications services in publicly accessible private communications networks), *also* any other data controller, for example, a company providing security products and services or e-commerce providers, would be entitled to process traffic data for security purposes (if the requirements were met).

- This would mean that different actors/data controllers would be processing traffic data on the basis of different articles of the ePrivacy Directive: 4.1 for PECS *and* providers of publicly available electronic communications services in publicly accessible private communications networks and 6.6(a) for any other type of data controller.

- It follows from the above that the enlargement of the ePrivacy Directive does not affect Article 6.6 (a), except that its scope would no longer include providers of publicly available electronic communications services in publicly accessible private communications networks[3]. Furthermore, the enlargement of the ePrivacy Directive does not in any way entail the need to adopt Article 6.6 (a). Moreover, the problems of

[1] Providers of publicly available electronic communications services in public communications networks.

[2] The Article 29 Working Party confirmed that Article 4.1 of the ePrivacy Directive could be used to legitimize the processing of traffic data by telecoms and email providers not only for the purposes of preventing threats to the security of their services but also to avoid or minimize spam and viruses. See its Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21. 02.2006.

[3] Insofar as such providers would be covered by Article 4.1 and would be entitled to process traffic data, within certain limits, on the basis of Article 4.1 of the ePrivacy Directive as described above.

Article 6.6(a) described in my Second Opinion on the ePrivacy Directive remain, independent of the enlargement of the scope of the ePrivacy Directive. Adoption of Article 6.6 (a) would also risk creating confusion in view of the important role of Article 6 as currently formulated.

II. SCOPE OF SECURITY BREACH TO INCLUDE E-COMMERCE PROVIDERS AND ITS RELATION WITH ARTICLE 6.6 (a)

- If the scope of application of the security breach provisions is broadened as proposed by the EP, this would mean that, in addition to PECS[4], also e-commerce providers will have to notify security breaches.

- Because the widened scope to include e-commerce providers is limited to the security provisions of the ePrivacy Directive, such enlarged scope *per se* does not change the scope of application of other articles of the ePrivacy Directive. The other articles of the ePrivacy Directive remain applicable to PECS only, unless for very specific cases such as the spam provisions[5]. In other words, not because e-commerce providers are bound by the security provisions, they will be automatically covered by the remaining articles of the ePrivacy Directive.

- It follows from the above that enlarging the scope of the security breach provisions will not affect either the scope of the existing articles of the ePrivacy Directive or the scope of a potential Article 6.6 (a). I do not see any implications for Article 6.6.(a) derived from the enlargement of the security breach provisions to cover e-commerce providers. Furthermore, such enlargement does not create a need for 6.6 (a).

I hope the above is useful for you. If you need further advice, I remain at your disposal.

Best regards,

(signed)

Peter HUSTINX

Cc: Mr M. Harbour (MEP)

[4] As well as providers of publicly available electronic communication services in publicly accessible private networks (such as providers of Internet access in Internet cafes, Wi-Fi spots available in hotels, airports) if the overall scope of the ePrivacy is amended to include them.
[5] As well as Article 5 which also has a wider scope application.