EUROPEAN DATA PROTECTION SUPERVISOR

PETER HUSTINX
SUPERVISOR

Mr Bernd LANGEHEINE
Director B-Head of Unit (acting) B.1
DG INFSO
European Commission
B - 1049 Brussels

Brussels, 06 October 2010
PH/RB/et/D(2010)1516 **C 2010-0645**

Dear Mr Langeheine,

I am writing to contribute to DG INFSO's public consultation on open Internet and net neutrality in Europe. We understood from your services that this contribution will still be taken into account despite the fact that the deadline for contributions expired last week.

Net neutrality raises data protection and privacy issues. As you may be aware, pursuant to Regulation (EC) No 45/2001[1], the European Data Protection Supervisor ('EDPS') is competent to advise the EU institutions and bodies on data protection/privacy issues in a range of policy areas. These comments should be understood in the light of this role and focus on the current INFSO public consultation, which may lead to future policy actions in the area of net neutrality.

The EDPS services remain available, should you need any clarification in relation to these comments.

Yours sincerely,

(**signed**)

Peter Hustinx

[1] Regulation (EC) No 45/2001 of 18 December 2010 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

EDPS COMMENTS ON NET NEUTRALITY AND TRAFFIC MANAGEMENT

Contribution to DG INFSO's public consultation on open Internet and net neutrality in Europe

I. Background

1. Providers of electronic communication services such as ISPs may engage in 'traffic management'. Depending on the traffic management mechanisms used, they may examine the content of communications, including URLs visited, information downloaded (movies, music), email communications etc. with a view to potentially treating each communication differently, usually by attributing different quality or speed levels.

2. These activities are carried out using technologies that enable the examination of the digital packets that make up a message or transmission over a network. The initial examination enables the provider, depending on the content, to give a certain priority level to each type of digital packet, or simply block it. Obviously, the digital packets that make up a message or a transmission are related to a particular user insofar as each digital packet has the IP address of the originator and of the recipient.

3. The reasons for traffic management, treating each package differently, may be multiple. It may happen that the demand for the available bandwidth exceeds the capacity of the network. This may cause degradation of the service. To solve this problem, certain traffic may be prioritized or other traffic delayed, to ensure a certain quality of service particularly with respect to time-sensitive data. Traffic management may also be used to provide particularly high quality or reliability that is necessary in certain services. Differentiation may also be carried out for security purposes, e.g. searching for viruses, malicious code or spam, or to filter certain illegal content. Traffic management could potentially be used to discriminate in favour of those content providers willing to pay higher rates (to keep high speed levels).

4. The EDPS notes that the implementation of traffic management policies may require the monitoring of users' personal information, in particular their traffic and content data. This raises serious data protection and privacy issues. Regrettably, the questionnaire that serves as a background for the public consultation on open Internet and net neutrality does not refer to data protection and privacy, which as further explained below, should be considered carefully when the Commission develops policies on these issues.

II. Traffic management mechanisms: data protection/privacy implications

5. From a data protection/privacy perspective, two aspects related to the implementation of traffic management mechanisms are particularly important: **First,** the providers' ability to examine the content of messages or transmissions and, **second**, the possibility to attribute this information to a particular user. Traffic management mechanisms have the potential to collect both content and traffic data pertaining to individual users. Altogether, as further illustrated below, the potential impact on the protection of personal data and privacy of individuals of this activity could be considerable.

6. By intercepting traffic data, traffic management mechanisms may breach the confidentiality of communications, which is a fundamental right, guaranteed by Article 8

of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR') and Article 7 and 8 of the Charter of Fundamental Rights of the European Union (the "Charter") . Confidentiality is further protected in secondary EU legislation, namely, Article 5 of the ePrivacy Directive [2]. This article provides that "*Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality*".

7. Moreover, the implementation of such policies puts providers in a position to collect vast amounts of personal data, potentially affecting millions of users; furthermore, the collection and further processing of these data are particularly invasive if one takes into account that they could include records of every user's activity on the Internet - movies downloaded, emails exchanged, searches, etc.

8. **Taking this into account, the EDPS insists that privacy and data protection aspects must be taken into account by the Commission when considering policies on net neutrality and traffic management. Particular attention should be paid to the legal framework outlined below.**

III. The current data protection/privacy framework applying to traffic management

a) The existing EU legal framework

9. EU law provides data protection and privacy safeguards in the context of the confidentiality of communications. In considering EU policy developments on traffic management, it is important to recall this EU legal framework. In particular, Article 5.1 of the ePrivacy Directive which concerns the confidentiality of communications and requires consent to enable "…*listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users,* …". Also relevant is Article 6.1 which establishes that traffic data must be erased as soon as storage is no longer needed for purposes related to the communication itself (including billing purposes).[3] Exemptions to these provisions are subject to strict conditions.

10. In discussing the use of traffic management mechanisms, Recital 28 of the Universal Service and Citizens Rights Directive[4] explicitly refers to this legal framework as applying to traffic management mechanisms: "*Users should in any case be fully informed of* ***any limiting conditions imposed on the use of electronic communications services by the service and/or network provider****. Such information should, at the option of the provider, specify the type of content, application or service concerned, individual applications or services, or both.*" It then specifies that: "*Depending on the technology used and the type of limitation, such limitations may*

[2] 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.

[3] Compare also the Commission's recent proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA, COM(2010) 517 final. Article 6 of the proposal would make interception of data transmissions a criminal offence.

[4] Directive 2009/136/EC of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services.

require user consent under Directive 2002/58/EC (Directive on privacy and electronic communications)."[5]

b) The application of the framework to traffic management mechanisms

11. In line with the above, if providers of electronic communication services implement traffic management policies which constitute interception or surveillance of communications, Article 5 of the ePrivacy Directive would apply and require informed consent from the users concerned, i.e. from all those party to the communication. Whereas transparency (and information to individuals) is a key element for the protection of the personal data and privacy of individuals, it is not in itself sufficient. As further described below, after being informed, individuals must accept, i.e. consent to have their content and traffic data processed for the purposes sought by the traffic management policies implemented by the provider.

12. Consent to intercept communications and thus process personal data must be interpreted in the light of Article 2 (h) of the Data Protection Directive[6]. According to that Article, for consent to be valid it must be a freely given, specific and informed indication of the individual's wishes by which he signifies his agreement to personal data relating to him being processed. Recital 17 of the ePrivacy Directive re-affirms this *"(…) Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user's wishes, including by ticking a box when visiting an Internet website."*

13. Consent given on the occasion of the general acceptance of the terms and conditions governing the possible main contract (e.g. a subscription contract, in which consent is also sought to allow traffic management and thus a breach of the confidentiality of communications) must respect the requirements in the Data Protection Directive, that is, be informed, specific and freely given.

14. In practical terms this requires at least*:*

    a) the provision of sufficient information to the users;
    b) the use of appropriate language to ensure that they understand what they are consenting to and for what purposes. The use of overly complicated legal or technical jargon would not meet the requirements of the law;
    c) the information provided to users should be clear and sufficiently conspicuous so that users can not overlook it. This calls for the use of targeted means such as specific consent forms (rather than inserting the information in the general conditions of the contract and requiring a signature of the contract as such);
    d) the purposes of the traffic management policies/mechanism should be sufficiently specified. If the purposes sought by the traffic management are not sufficiently

---

[5] In some, limited cases consent may not be necessary. This derives from Article 4 of the e-Privacy Directive which provides that "The provider of a publicly available telecommunications service must take appropriate technical and organizational measures to *safeguard security of its services, if necessary in conjunction with the provider of the public telecommunications network with respect to network security"*. In interpreting this provision, the Article 29 Working Party stated that the setting up and use of filtering systems by email providers for the purposes of detecting virus might be justified by the obligation to take appropriate technical and organization measures to safeguard security of their services as foreseen in Article 4 of the e-Privacy. See Working Party Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006.

[6] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

specified, for example, in an attempt to maintain the provider's ability to use the data for different purposes, this would not meet the legal standards either.

e) Finally, consent under the applicable legal framework also requires an affirmative action by the user to signify his/her agreement. Implied consent would not meet this standard.

15. In addition to the above, it is important to highlight that for consent to be freely given, users should have the possibility to make a real choice whether or not to consent. A potential problem for users to be able to make such choice would arise if *all* providers in a given market engaged in traffic management. This would mean that users not willing to consent to have their data monitored would have no alternative service/choice in the market place. The only option left for them would be not subscribing to an Internet service at all. Internet is playing an increasingly central role in people's lives. Given that the Internet has become an essential tool both for work and for private purposes, not subscribing to an Internet service does not constitute a valid alternative. The consequence would be that the individuals would have no real choice, i.e. they would not be able to freely give consent. The EDPS urges the Commission to take this into account, particularly if this scenario is a likely one (i.e. that all providers are engaged in traffic management). A possible solution to this problem would entail requiring providers to offer an alternative service, for example, an Internet subscription not subject to traffic management.[7]

16. Last but not least, personal data retained in the context of using traffic management technologies must also respect other principles that derive from the Data Protection and ePrivacy Directives. These may be highly relevant depending on the policies under consideration, but do not need to be discussed at this stage.

17. In summary, the EU data protection framework provides data protection and privacy safeguards in the context of the confidentiality of communications, which should be maintained in future policy developments on net neutrality and traffic management.

IV. Recommendations

18. In light of the above, the EDPS recommends that in presenting any policies on net neutrality and particularly on traffic management, the Commission should:

a) Take into account data protection and privacy issues together with other existing rights and values;

b) Preserve the existing data protection/privacy legal framework, namely the requirement that traffic management mechanisms that enable the examination of communications (content and traffic) are only allowed if the users concerned have provided informed, specific and free consent.

Brussels, 6 October 2010

[7] An additional issue not discussed here relates to the feasibility to obtain consent from ***all*** users involved in a communication, as required under Article 5.1. This is because obtaining the consent of all users requires not only obtaining the consent of the subscriber but also of the sender (who may or not be a subscriber). It is uncertain how this could be implemented in practice.