EUROPEAN DATA
PROTECTION SUPERVISOR

EDPS COMMENTS ON SELECTED ISSUES THAT ARISE FROM THE IMCO REPORT ON THE REVIEW OF DIRECTIVE 2002/22/EC (Universal Service) & DIRECTIVE 2002/58/EC (ePrivacy)

I. INTRODUCTION

1. Generally speaking, the EDPS views the amendments adopted in the IMCO Report favourably. For example, the EDPS is particularly pleased about the inclusion of companies operating on the Internet under the scope of the obligation to notify security breaches. He is also pleased with the amendment that enables legal and natural persons to file legal actions for infringement of any provision of the ePrivacy Directive (not only spam). He strongly hopes that the plenary vote of the European Parliament will maintain these amendments[1].

2. However, the EDPS has some observations about *ad hoc* amendments that may weaken the protection of personal data and privacy of individuals using the Internet. Some of the amendments that cause concern are related to traffic data and the protection of intellectual property rights, as well as regulation of notification of security breaches. Yet, the present comments are limited to those issues for which the EDPS advice has been explicitly requested, and which were not covered by the previous EDPS Opinion on the review of the ePrivacy Directive[2], namely, traffic data and the protection of intellectual property rights.

II. ANALYSIS OF IMCO AMENDMENTS RELATED TO IP ADDRESSES

3. A question arises as to whether Internet Protocol ("IP") addresses are personal data. This is relevant because both the ePrivacy Directive and the Data Protection Directive[3] apply whenever personal data are processed. If IP addresses are not deemed personal data, they can be collected and further processed without the need to fulfil any legal obligation arising from the two above mentioned Directives. For example, such outcome would enable a search engine to store, for an indefinite period, IP addresses assigned to accounts from which, for example, materials related to a specific health condition (e.g. AIDS) have been searched.

---

[1] In order to include companies operating on the Internet under the scope of the obligation to notify security breaches, the IMCO Report has included in various amendments an explicit reference to companies operating on the Internet alongside providers of electronic communications services. In particular, the amendments where such reference has been added include the following: Amendments 33, 123, 124, 126 and 136. In order to provide for civil law remedies for any legal person to fight infringements of any of the provisions of the ePrivacy Directive, the IMCO Report has adopted amendment 133.

[2] EDPS Opinion of 10 April 2008 on the Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[3] Directive 95/46/EC 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.

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 63
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

4. Amendment 30 of the IMCO Report deals with IP addresses. Among other things, the amendment establishes the circumstances under which IP addresses should be considered personal data. It, therefore, also establishes, *a contrario*, when such information should not be deemed personal data. Amendment 130 of the IMCO Report deals with the processing of traffic data, which includes IP addresses.

5. The EDPS considers that Amendment 30 should not establish by definition when IP addresses are personal data. In addition, rather than addressing this issue immediately through legislation, given the complexity of the subject matter and its fact-intensive nature, he believes that a thorough study and report should be made of the issues. Amendment 130 also should be deleted or, alternatively, narrowly defined.

II.1. IP addresses: the technical and legal background

6. IP addresses are essential to the working of the Internet. They identify network participating devices, such as a computer by a number. Every time that an individual goes onto the Internet using an Internet access device, for example to surf the Web, the Internet service provider ("ISP") attributes an IP address to the device he is using. An IP address looks like a string of numbers separated by dots, such as 122.41.123.45.

7. The IP address that the ISP attributes to an individual may always be the same for every time he surfs the Internet (referred to as static IP addresses). Other IP addresses are dynamic, meaning that the Internet access provider attributes a different IP address to its customers every time they connect to the Internet. Obviously, the ISP can connect the IP address to the subscriber's account to whom they have assigned the (dynamic or static) IP address.

8. Article 2 (a) and Recital 26 of the Data Protection Directive[4] contain a definition of personal data. Whether a piece of information, in this case an IP address, constitutes personal data or not must be assessed on a *case-by-case* basis, applying the definition provided in this legal framework. The Article 29 Working Party[5] issued an opinion on the definition of personal data[6] to help stakeholders carry out assessments as to whether information meets the requirements to be considered "personal data" and must be, therefore, collected and further processed under the conditions of the Data Protection and ePrivacy Directives.

9. In different opinions, the Article 29 Working Party has identified many cases where IP addresses are personal data[7]. For example, it considered IP addresses collected to enforce intellectual property rights (i.e. identify Internet users who are alleged to have violated intellectual property rights) to be personal data insofar as they are used for enforcement

---

[4] Under Article 2(a) "*personal data shall mean any information relating to an identified or identifiable natural person (data subject); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, psychological, mental, economic, cultural, or social identity*". Recital 26 says: " *Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable;* .....".

[5] This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

[6] Working Party Opinion 136 on the concept of personal data, adopted on 20 June 2007.

[7] For example, Working document 37 "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection, adopted on 21 November 2000 and Working Party Opinion 136 on the concept of personal data, adopted on 20 June 2007.

of such rights against a given individual.[8] Yet, it has acknowledged that, in some cases, IP addresses may not be personal data. The EDPS fully endorses these views.

II.2. Comments on IMCO Amendments

(a) Definition of personal data for IP addresses

10. Amendment 30 of the IMCO Report incorporates Recital 28(a) of the ePrivacy Directive. It reads as follows: "*For the purpose of Directive 2002/58/EC, Internet Protocol addresses should be considered as personal data only if they can be directly linked to an individual alone or in conjunction with other data. By ...+, the Commission should propose specific legislation on the legal handling of Internet Protocol addresses as personal data within the framework of data protection following consultation of the Article 29 Working Party and the European Data Protection Supervisor.*"

11. The content of Amendment 30 is twofold: first, it establishes a standard for the determination of whether IP addresses must be deemed personal data (only if they can be directly linked to an individual alone or in conjunction with other data). The standard created is, arguably, slightly different from the standard embodied in the definition of personal data contained in Article 2(a) and Recital 26 of the Data Protection Directive, affording, possibly, more limited protection because the scope of Article 2(a) seems broader.[9] Second, it imposes upon the Commission an obligation to propose legislation regarding the legal handling of IP addresses.

12. Unless there are sound reasons that justify otherwise, the EDPS considers that it is inappropriate to legislate on whether a given piece of information is or not personal data. As pointed out above under II.1, Article 2(a) and Recital 26 of the Data Protection Directive already contain a definition of personal data, providing the tools for stakeholders, and eventually judicial review, to establish under the circumstances of a particular case whether any piece of information is or is not personal data. More importantly, considering that such assessments are factual in nature and based upon current technologies, which are rapidly evolving, it seems inappropriate to address this question through a Directive, which takes time to adopt and implement, and which will quickly be outpaced by new circumstances.

13. In addition to the above, the EDPS considers that it is not appropriate to create new definitions of personal data that may *differ* from the general one provided in the Data Protection Directive. Such an approach could lead to a piecemeal framework where different pieces of information would be subject to different standards. There is no justification for this, and it would only serve to create confusion.

14. In the case of IP addresses, the EDPS considers that there is no evidence justifying that the existing definition of personal data as provided in Article 2(a) of the Data Protection Directive and interpreted by the Article 29 Working Party and judicial review does not work for the purposes of assessing whether IP addresses are personal data or not in the light of the specific facts surrounding their collection. These views are shared by the Article 29 Working Party.[10] Furthermore, if IP addresses of Internet users are deemed

---

[8] Working Party Document 104 on data protection issues related to intellectual property rights, adopted on 18th January 2005.

[9] Under Article 2(a) an identifiable person is the one who can be identified, directly or indirectly. Recital 30 does not include the wording "indirectly". It does not include either the need to take into account for the purposes of determining whether a person is identifiable *"all the means likely reasonably to be used either by the controller or by any other person to identify the said person"* as established under Recital 26 of the Data Protection Directive.

[10] See letter dated 5 May 2007 from the Chairman of the Article 29 Working Party to Mr. Gérard DEPREZ, Chairman of the LIBE Committee, on IP addresses.

personal data in more limited occasions, and their collection and use are less restricted due to a narrower definition of personal data, such an approach could foster a surveillance society. For the above reasons, **the EDPS suggests deleting the first sentence of Amendment 30 of the IMCO Report.**

15. For the same reasons as outlined above, it seems illogical for the second sentence of Amendment 30 to impose an obligation upon the Commission to propose legislation on IP addresses: if there is no evidence that such legislation is needed, why would the Commission be obligated to propose it? The EDPS concedes that, in the future, it may be helpful to reflect upon this issue, envisaging the different scenarios in which IP addresses are used and assessing the effects of the applicable legal regime. Given that this is a complex technical and legal issue, an in-depth study would be highly beneficial.

16. **For this reason, the EDPS would welcome that Amendment 30 of the IMCO Report be amended to establish the need to commission a study on the subject.** An amendment along the following lines could serve this purpose: *No later than XX 1, the Commission shall submit to the European Parliament, the Council, and the European Economic Social Committee a study and a report with recommendations on standard uses of IP addresses and the application of the ePrivacy and Data Protection (95/46/EC) Directives to their collection and further processing, following the consultation of the EDPS, the Article 29 Working Party, and other stakeholders to include industry representatives.*

(b) The processing of traffic data, including IP addresses for security purposes

17. Amendment 130 of the IMCO Report creates a new Article 6a in the ePrivacy Directive which relates to the processing of traffic data for security purposes. Amendment 130 reads as follows: *"Traffic data may be processed by any natural or legal person for the purpose of implementing technical measures to ensure the security of a public electronic communication service, a public or private electronic communications network, an information society service or related terminal and electronic communication equipment. Such processing must be restricted to that which is strictly necessary for the purposes of such security activity."*

18. The EDPS understands that the goal of this Amendment is to enable security service providers to collect and further use IP addresses for security purposes. This Amendment is aimed at establishing what is referred to as "legal grounds" authorizing the collection of traffic data. Without this Amendment, the collector of IP addresses deemed personal data would be subject to Article 7 of the Data Protection Directive, which requires legal grounds to justify the processing, as well as Article 5 of the ePrivacy Directive, which establishes the confidentiality of traffic data.[11] Therefore, this Amendment legitimizes the collection of IP addresses for security purposes. Of course, this Amendment does not exempt the processing of traffic data for security purposes from compliance with the other provisions of the ePrivacy and Data Protection Directives, which will still apply.

19. The EDPS fully recognizes the need to secure the Internet and the need for companies to engage in certain activities to meet this purpose. Such activities may include preventing

[11] Examples of legal grounds set forth under Article 7 include grounds allowing the processing of data when the processing is necessary for the performance of a contract to which the data subject is party (sub b), and when necessary for the performance of a task carried out in the public interest (sub e). It also includes sub (f) the processing when necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article (1).

unauthorized access and malicious code distribution, stopping the denial of service attacks, and damages to computer and electronic communications systems[12].

20. The EDPS understands that some of these activities may entail the processing of certain traffic data, including IP addresses. In this regard, he is not against the setting up of a favorable legal framework such as that embodied in Amendment 130 enabling such security service providers to collect certain traffic data for security purposes, subject to the application of the provisions of the Data Protection and the E-privacy Directives.

21. Nevertheless, because the Amendment is broadly constructed, for example, it does not define what should be understood by security and it does not limit the type of entities (data controllers) it is meant to apply, the EDPS is concerned that it could be interpreted too broadly. In particular, the EDPS is concerned that it could be used to legitimise the collection of traffic data for purposes that are not purely security related. He is also concerned that it could open the door for anyone, not only providers of security services and products, to process traffic data alleging to do it for security purposes.

22. In balancing on the one hand the justifications for this provision and on the other the privacy risks derived from an overly broad interpretation as illustrated above, the EDPS advises **against the adoption of this Amendment**.

23. However, **if it were to be adopted, it should be narrowly constructed to include various safeguards. Towards this end, Amendment 130 should be modified as follows:**

24. **First, it should be preceded by the following phrase to ensure that the other requirements of the Data Protection Directive still apply (e.g. data subject rights, accountability, enforceability): "*Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive* *(t)raffic data may be processed by .....*"** This means that all currently applicable data protection safeguards will continue to apply.

25. **Second, the reference to "*any natural or legal person*" should be replaced by "providers of security services"** to avoid giving a carte blanche authority to process personal data to entities that are not engaged in the promotion of the security of the Internet.

26. **Third, it should be accompanied by a definition of the term "security"** to help prevent this Amendment from being used as a justification for processing traffic data for goals other than purely pursuing security. In line with the above, to help address this issue, the EDPS suggests using the following definition of the term network and information security from Article 4(c) of the Regulation establishing the European Network an Information Security Agency (ENISA)[13]: *"the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems"*

---

[12] See the threats identified in the Council Framework Decision 2005/222JHA of 24 February 2005 on attacks against information systems, particularly 2 (illegal access to information systems), Article 3 (illegal system interference), Article 4 (illegal data interference) and 5 (instigation, aiding and abetting and attempt).

[13] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

27. **Fourth**, the EDPS suggests that **a recital be added to illustrate the types of processing that would be covered** under the Amendment and to encourage ENISA's involvement in their determination. The recital could read as follows: "*The processing of traffic data for security purposes will enable the processing of such data by providers of security services acting as data controllers for the purposes of preventing unauthorized access and malicious code distribution, stopping the denial of service attacks, and damages to computer and electronic communications systems. ENISA should publish regular studies with the purpose of illustrating the types of processing allowed under Article X of the ePrivacy Directive*".

III. ANALYSIS OF IMCO AMENDMENTS DIRECTLY OR INDIRECTLY RELATED TO THE GRADUATED RESPONSE SCHEMES

28. A question has arisen as to whether some of the amendments contained in the IMCO Report may lay down the grounds for allowing widespread monitoring of individuals' usage of the Internet and associated filtering techniques for the purposes of detecting alleged copyright violation. In particular, it has been suggested that some of the amendments support the setting up of schemes usually referred to as a "graduated response" or "3 strikes approach," briefly described below.

29. In a nutshell, under such types of schemes ("graduated response" or "3 strikes approach"), copyright holders would identify alleged copyright infringement by engaging in systematic monitoring of Internet users' activities. After identifying Internet users alleged to be engaged in copyright violation by collecting their IP addresses,[14] copyright holders would send the IP addresses of those alleged to be engaged in copyright violation to the Internet Service Provider who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the ISP three times would result in the ISP's termination of the subscriber's Internet connection.

30. The EDPS does not support a legal framework that allows the systematic monitoring of Internet users' activities. As further developed below, such a framework is highly invasive of an individual's private sphere and also jeopardises freedom of speech. To avoid this outcome, the EDPS suggests making some adjustments to Amendment 9 and adding a recital to clarify that cooperation procedures should not allow for the systematic and proactive surveillance of Internet usage.

III.1. Systematic monitoring of Internet use and the need for a balanced approach

31. The EDPS is aware of the importance of enforcing intellectual property rights and believes that a balance needs to be struck between the legitimate objective of fighting against illegal content and the means used to do so. A balanced approach must necessarily take into consideration the *necessity* and the *proportionality* principles of data protection legislation. Whereas a necessity test may conclude that the monitoring of a *single* individual suspected of engaging in violation of copyright may be necessary, the systematic, proactive surveillance and filtering of law abiding regular Internet users would clash with the necessity principle.

[14] For example, copyright have used techniques such as automated search engines to trace alleged piracy activities. Once alleged piracy activities have been found, the IP address of the individual alleged to be engaged in such activities is collected in order to ascertain the name of the individual who holds such IP address, which is in the possession of the Internet Access provider. Also, copyright holders pose as file sharers in Peer-to-peer networking to identify file sharers that allegedly exchange copyright material.

32. The proportionality principle[15] requires personal data collected and further processed to be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed. Considering: 1) the fact that such monitoring would affect *all* users, irrespective of whether they are under suspicion, 2) the potential *effects* of the monitoring , which could result in disconnection of Internet access, and 3) the fact that the entity making the assessment and taking the decision will typically be a private entity (i.e. the copyright holders or the ISP), it seems clear that these types of schemes do not comply with the proportionality principle, which is fundamental to data protection.

33. In its opinion of 18 January 2005, the Article 29 Working Party, discussing this issue,[16] stated that "*While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet (...). Such investigation falls within the competence of judicial authorities.*"

34. Consistent with the Article 29 Working Party, the EDPS has already highlighted[17] that clearly these types of monitoring schemes raise concerns about private sector (e.g. ISPs' or copyright holders') control over the content of telecommunications, an area that is in principle under the competence of law enforcement authorities.

35. In sum, data protection principles call for a graduated approach whereby monitoring may be lawful in the context of limited, specific, ad hoc, situations whereby well-grounded suspicions of copyright abuse, preferably at a commercial scale, exist. In such cases, the collection of information demonstrating alleged Internet abuse may be deemed necessary and proportional for the purposes of preparing the legal proceedings, including litigation. However, these principles are not respected in instances that entail widespread, systematic, proactive monitoring of the use of Internet by alleged or "would be" infringers.

36. Finally, in this context it is worth recalling the European Parliament's resolution stressing the need for a solution in compliance with the fundamental rights of individuals, avoiding the adoption of "measures conflicting with civil liberties and human rights and with the principles of proportionality, effectiveness and dissuasiveness, such as the interruption of Internet access".[18]

III.2. Comments on IMCO Amendments

37. The EDPS has identified the following amendments to Directive 2002/22/EC as provisions that are or may be related to the subject at issue, i.e. the setting up of a surveillance scheme with the purposes of fighting alleged copyright violations: Amendment 9, creating Recital 12c;[19] Amendment 76, creating Article 21 paragraph 4a;[20] and Amendment 112, creating Article 33 paragraph 2a.[21]

---

[15] Article 6 (1) c of the Data Protection Directive

[16] Working Party Document 104 on data protection issues related to intellectual property rights, adopted on 18 January 2005.

[17] EDPS Opinion of 23 June 2008 on the Proposal for a Decision establishing a multi-annual Community programme on protecting children using the Internet and other communication technologies.

[18] European Parliament resolution of 10 April 2008 on cultural industries in Europe (2007/2153(INI))

[19] "*In order to address public interest issues with respect to the use of communications services, and to encourage protection of the rights and freedoms of others, the relevant national authorities should be able to produce and have disseminated, with the aid of providers, information related to the use of communications services. This information should include warnings regarding copyright infringement, other unlawful uses and dissemination of harmful content, and advice and means of protection against risks to personal security, which may for example arise from disclosure of personal information in certain circumstances, privacy and personal data. The information could be*

38. What is *the basic message or intention* of these amendments? Amendments 9 and 76 require national authorities to work with electronic communications services, such as Internet access providers, to develop and provide public interest information to subscribers. Amendments 9 and 76 provide some examples of the types of information to be provided, which include "*infringements of copyright and related rights*" and "*warnings regarding copyright infringement.*" Regarding the *timing* for delivery of such information, Amendment 9 states that "*it should be produced either as a preventative measure or in response to particular problems.*"

39. Amendment 112 sets up a coordination procedure by requiring national regulatory and other authorities to promote the cooperation between providers of electronic communications services and representatives of content providers. An example of such cooperation includes the development and distribution of public interest information to subscribers. In setting up the above obligations,[22] Amendments 9, 76 and 112 are vague and subject to varying interpretation.

40. At the outset, the EDPS notes that he is generally supportive of cooperation procedures between the copyright and telecommunication industries, and believes such cooperation is important to ensure the proper workings of the Internet. Against this backdrop, the EDPS makes the following observations regarding whether the proposed amendments create a "3 strikes approach:"

41. First, the amendments do not explicitly create a surveillance system, enabling the copyright industry to monitor Internet usage and filtering of IP addresses pertaining to Internet users alleged to be engaged in copyright violation. Yet, if Amendments 30 and 130 discussed under section II were to be adopted in their current versions, they would facilitate copyright holders' ability to routinely monitor the IP addresses of Internet users, which could be used to facilitate a "3 strikes approach" scheme.

---

coordinated by way of the cooperation procedure established in Article 33(2a) of Directive 2002/22/EC. Such public interest information should be produced either as a preventative measure or in response to particular problems, should be updated whenever necessary and should be presented in easily comprehensible printed and electronic formats, as determined by each Member State, and on national public authority websites. National regulatory authorities should be able to oblige providers to disseminate this information to their customers in a manner deemed appropriate by the national regulatory authorities. Significant additional costs incurred by service providers for dissemination of such information, for example if the provider is obliged to send the information by post and thereby incurs additional postage costs, should be agreed between the providers and the relevant authorities and met by those authorities. The information should also be included in contracts."

[20] *"Member States shall ensure that national regulatory authorities oblige the undertakings referred to in paragraph 4 to distribute public interest information to existing and new subscribers where appropriate. Such information shall be produced by the relevant public authorities in a standardised format and shall inter alia cover the following topics: (a) the most common uses of electronic communications services to engage in unlawful activities or to disseminate harmful content, particularly where it may prejudice respect for the rights and freedoms of others, including infringements of copyright and related right, and their consequences; and (b) means of protection against risks to personal security, privacy and personal data in using electronic communications services. Significant additional costs incurred by an undertaking in complying with these obligations shall be reimbursed by the relevant public authorities"*

[21] *"2a. Without prejudice to national rules in conformity with Community law promoting cultural and media policy objectives, such as cultural and linguistic diversity and media pluralism, national regulatory authorities and other relevant authorities shall as far as appropriate promote cooperation between undertakings providing electronic communications networks and/or services and the sectors interested in the promotion of lawful content in electronic communication networks and services. That co-operation may also include coordination of the public interest information to be made available under Article 21(4a) and Article 20(2)."*

[22] These obligations could be summarised as follows: (i) National authorities should produce information which among others will contain warnings about copyright infringements; (ii) National authorities are encouraged to set up a cooperation procedure between the telecommunications industry and the copyright industry; the scope of which should include the determination of information (referred to under i) to be delivered to subscribers, and (iii) National authorities will have the competence to oblige electronic communication services such as Internet access providers to deliver to their subscribers the information agreed under (i) and (ii).

42. Second, the amendments do not explicitly provide for a coordination scheme pursuant to which the copyright industry could collect IP addresses of alleged infringers and provide them to telecommunications industry. The aim of the cooperation scheme set up by the amendments is, among others, to determine which types of public interest information, including those that are copyright related, must be disseminated to subscribers. The type of information seems to be general in nature, for example, information about the existence of a Web site that promotes unlawful sharing of copyright information. Although it does not seem to be information related to particular alleged infringements, this is not entirely clear.

43. In sum, it seems fair to say that the amendments do not set up unequivocally a "3 strikes approach" system. They do not spell out thoroughly the details of such a system. However, in the EDPS' view, these amendments provide for a "slippery slope," and can be interpreted as erecting the foundations for such a system and even favouring its emergence, to be further developed either at national or EU levels.

44. The EDPS understands that it is also not the purpose of these amendments to create a "3 strikes approach" system. However, in light of the points above, **this should be clarified in a recital,** which could read as follows: *"Cooperation procedures created pursuant to this Directive should not allow for systematic and proactive surveillance of Internet usage."*

45. **In addition, the EDPS also recommends deleting Amendment 9 altogether, or alternatively redrafting it** to account for the following: 1) in the first sentence, add the qualifying phrase "public interest" to the word "information"; 2) in the second sentence, the word "warnings" should be clarified to ensure that they are "public interest warnings"; 3) remove the reference to "*a response to particular problems,*" which also evokes individual, rather than more generalized warnings.

IV. ANALYSIS OF IMCO AMENDMENTS RELATED TO STANDARDISATION TOWARDS THE DETECTION, INTERCEPTION AND PREVENTION OF INFRINGEMENTS OF INTELLECTUAL PROPERTY RIGHTS

46. The question has also arisen whether some amendments adopted by the IMCO Report may encourage the control of the users' Internet activities. This may be done by enabling Member States to issue standards for electronic communications equipment in order to control the content, mostly copyright, accessed or used by Internet users. The technical means allowing such control are usually referred to as digital rights management systems ("DRM"). For example, DRM technologies can control file access (number of views, length of views), altering, sharing, copying, printing, and saving. These technologies may be contained within the operating system, program software, or in the actual hardware of a device.

47. The above-mentioned effects are supposed to be achieved by Amendment 134, which modifies Article 14(1) of the ePrivacy Directive regarding standardisation and also through Amendment 81 which modifies Article 22.3 of Directive 2002/22/EC. This section analyses both amendments and assesses their effects, and concludes that both amendments should not be adopted without further analysis and exploration.

IV.I. Standardisation for the purposes of designing privacy-friendly products

48. The enforcement of data protection obligations is sometimes more difficult in the Internet age and is made easier if information technology products are designed and built with legal requirements in mind at the outset. This approach ensures that data are

processed in accordance with the law from the beginning, and removes the need for enforcement actions *a posteriori*.

49. Article 14 of the ePrivacy Directive deals with this issue and illustrates the concept of "privacy by design." In particular, it deals with standardisation to make privacy friendly products. The initial Commission's Proposal does not contain any amendment to this provision. In particular, Article 14(3) of the ePrivacy Directive provides that "*where required, measures may be adopted to ensure that the terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC.*" Article 14(1) establishes that such technical requirements should not impede the placing of equipment on the market and the free circulation of such equipment in and between Member States.

50. In sum, these Articles enable Member States to impose requirements for information technology products to meet certain standards that would ensure and facilitate the users' control of their personal data and thus compliance with the Data Protection Directives. In setting up standards, Article 14(1) requires Member States to ensure that these requirements do not prevent the placement of products on the market or inhibit free circulation in and between Member States.

IV.2. Comments of IMCO Amendments

51. Amendment 134 would modify Article 14(1) to include the following sentence, which appears in italics: "1. In implementing the provisions of this Directive, Member States shall ensure, subject to paragraphs 2 and 3, that no mandatory requirements for specific technical features, *including, without limitation, for the purpose of detecting, intercepting or preventing infringements of intellectual property rights by users,* are imposed on terminal or other electronic communication equipment which could impede the placing of equipment on the market and the free circulation of such equipment in and between Member States."

52. For the reasons outlined below, the EDPS advises against the adoption of this Amendment.

53. First, the content of the Amendment bears no relation to the subject matter - "privacy by design" - of the Article which it would amend. Indeed, as explained above, Articles 14(1) and 14(3) of the current ePrivacy Directive deal with standardisation of information technology products towards ensuring that they are built in a privacy-friendly way. These Articles are consistent with the overall subject matter of the Directive, which is focused on privacy in the electronic communications sector.

54. By contrast, the proposed Amendment 134 refers to standardisation for completely different purposes, i.e. for detecting, intercepting, or preventing infringements of intellectual property rights by users. This type of standardisation concerns the design of software and hardware products to enable copyright holders to easily monitor the use of their works and to detect copyright infringements and violations of license terms. It concerns the standardisation of digital rights management systems.

55. The EDPS believes that it does not make sense for Article 14, which is focused on standardisation for the purposes of enhancing data protection and privacy, to be expanded to include standardization for other, completely unrelated topics.

56. Second, by including in Article 14(1) the reference to standardisation for purposes of detecting, intercepting, or preventing infringements of intellectual property rights, this

Article recognises that Member States can impose standards in this area as well (not only for privacy purposes as stated in Article 14.3), provided that such standards ensure the free circulation of such equipment in and between Member States.

57. In this context, there is a question as to whether it is appropriate for Member States to require information technologies to meet certain standards, i.e. to incorporate certain features, to detect, intercept, or prevent infringements of intellectual property rights by users. Such measures, referred to as DRM, have a significant impact on the privacy of individuals insofar as they facilitate the monitoring of an individual's activities with respect to a particular copyrighted material. For example, it would enable the copyright holder to know which pages an individual views, copies, or transfers. A comparable example in the offline word would be if someone were able to monitor which pages of a magazine an individual views. If these measures were to be adopted, they should integrate data protection and privacy safeguards.

58. For the reasons outlined above, the adoption of any Amendment allowing for such measures should be preceded by a thorough exploration of the issues at stake in the right forum, including public consultation with the relevant stakeholders, which has not taken place at this stage. **Taking this into account, the EDPS does not believe that it is appropriate at this stage to adopt such measures.**

59. The EDPS notes another amendment, Amendment 81, which modifies Article 22(3) of Directive 2002/22/EC. This Amendment has a similar effect as Amendment 134 analysed above. Amendment 81 which appears in italics below recognises that "a national regulatory authority may issue guidelines setting minimum quality of service requirements, and, if appropriate, take other measures, in order to prevent degradation of service and slowing of traffic over networks, "*and to ensure that the ability of users to access or distribute lawful content or to run lawful applications and services of their choice is not unreasonably restricted.*"

60. The Amendment allows national authorities to issue guidelines to be imposed upon software and hardware products to enable the access or distribution of lawful content or applications. In other words, measures designed to prevent the access and distribution of unlawful content, including intellectual property, referred to above as DRM.

61. As is the case with Amendment 134, Amendment 81 also makes use of a provision of Directive 2002/22/EC related to a completely unrelated topic - the degradation of the service. The Amendment is focused on distribution of unlawful content, including intellectual property and is unrelated to degradation of service. As it was said above, in the light of the importance of the measures proposed and their direct impact on the privacy of individuals, **the EDPS advises against adoption of this Amendment prior to engaging in an in-depth, thorough analysis of its effects.**

V. CONCLUSION

62. The EDPS is concerned about some *ad hoc* amendments contained in the IMCO Report which, if adopted, would result in weakening personal data and privacy protections of individuals using the Internet. He is concerned with Amendments 9, 30, 76, 81,112 130, 134 of the IMCO Report related to the processing of traffic data and the protection of intellectual property rights.

63. While each of these amendments, taken individually, do not provide for the mass surveillance of Internet users, as a whole, the adoption of the set of amendments pointed out above would undoubtedly favour this outcome. Indeed, if the collection of IP addresses of Internet users would be subject to a more lenient legal regime, enabling their systematic processing (Amendments 30 and 130), if their routine transfer to ISPs would be allowed for the purposes of terminating subscribers' Internet connections (Amendments 9, 76 and 112) and if the adoption of technical standards for content filtering and monitoring would be favoured (Amendments 134 and 81), the net effect will be increased monitoring of Internet users' activities, which inevitably would infringe upon their data protection and privacy rights.

64. In order to avoid this undesirable effect and ensure the proper protection of the privacy and data protection rights of Internet users, the EDPS urges the European legislators to take the following into account:

65. **First, delete** the first sentence of Amendment 30 which establishes a separate standard for the determination of whether IP addresses must be deemed personal data. As pointed out in section II, this is unnecessary, unjustified and would only lead to confusion. For the same reasons, **modify** the second sentence of Amendment 30 which requires the Commission to propose legislation on IP addresses with the following: *"No later than XX 1, the Commission shall submit to the European Parliament, the Council, and the European Economic Social Committee a study and a report with recommendations on standard uses of IP addresses and the application of the ePrivacy and Data Protection (95/46/EC) Directives to their collection and further processing, following the consultation of the EDPS, the Article 29 Working Party, and other stakeholders to include industry representatives."*

66. **Second,** in the light of the privacy risks associated with a potentially over broad interpretation, **refrain** from adopting Amendment 130. Alternatively, **modify** Amendment 130 as follows: 1) **insert** the following phrase to ensure that the other requirements of the Data Protection Directive still apply: *"Without prejudice to compliance with the provisions other than Article 7 of Directive 95/46/EC and Article 5 of this Directive"*; 2) **replace** *"any natural or legal person"* with "providers of security services" to avoid providing carte blanche authority to process personal data to entities that may not be engaged in the promotion of Internet security; 3) **insert** the definition of network security contained in Article 4(c) of the Regulation establishing the European Network an Information Security Agency (ENISA); and 4) **add** a recital illustrating the types of processing that would be covered under the Amendment and encouraging ENISA's involvement in their determination: *"The processing of traffic data for security purposes will enable the processing of such data by providers of security services acting as data controllers for the purposes of preventing unauthorized access and malicious code distribution, stopping the denial of service attacks, and damages to computer and electronic communications systems. ENISA should publish regular studies with the purpose of illustrating the types of processing allowed under Article X of the ePrivacy Directive".*

67. **Third, clarify** in a recital that the intention of Amendments 9, 76 and 112 is not to enable the systematic monitoring of Internet users, to read as follows: *"Cooperation procedures created pursuant to this Directive should not allow for systematic and proactive surveillance of Internet usage."*

68. **Fourth, delete** Amendment 9 altogether insofar as its vagueness would favour its misinterpretation. Alternatively, **redraft** it taking the following into account: 1) in the first sentence, add the qualifying phrase "public interest" to the word "information"; 2) in the second sentence, the word "warnings" should be clarified to ensure that they are "public

interest warnings"; 3) remove the reference to "*a response to particular problems,*" which also evokes individual, rather than more generalized warnings.

69. **Fifth, refrain** from adopting Amendments 134 and 81. The adoption of technical measures requiring terminal equipment to incorporate certain features, to detect, intercept, or prevent infringements of intellectual property rights by users may have a significant impact on the privacy of individuals insofar as they facilitate the monitoring of an individual's activities with respect to a particular copyrighted material. The potential adoption of any Amendment allowing for such measures should be preceded by a thorough exploration of the issues in the right forum, to include public consultation with the relevant stakeholders, which has not yet taken place.

Brussels, 2 September 2008