EDPS COMMENTS ON DG CONNECT'S PUBLIC CONSULTATION ON "SPECIFIC ASPECTS OF TRANSPARENCY, TRAFFIC MANAGEMENT AND SWITCHING IN AN OPEN INTERNET"

The EU Commission has launched a public consultation aiming at obtaining input on specific aspects which emerged as key issues in the net neutrality debate that has taken place in Europe over the past years. A primary concern of the Commission's action in this field is to enable consumers to make informed choices in a competitive market governed by clear rules, through policy measures addressing the issues of transparency, switching and certain aspects of traffic management, including deep packet inspection (DPI).[1]

The EDPS welcomes the Commission's initiative to consult a wide range of interested parties, including private and public sector as well as civil society groups on the issues related to the net neutrality. The EDPS regards this consultation as an important part of the debate, which has to take place before any policy recommendations or legal measures are developed.

The EDPS takes note that the Commission's initiative follows up a Traffic Management Investigation carried out by the Body of European Regulators of Electronic Communications (BEREC)[2] undertaken upon the Commission's request.

I. Relevance of personal data protection in the context of the net neutrality debate

Traffic management practices, especially those involving the examination of citizen's communications on the Internet by means of DPI techniques, bear high risks for the privacy and the protection of personal data of individuals. By inspecting communications data, Internet Service Providers (ISPs) may interfere with individuals' privacy and breach the confidentiality of communications, which are fundamental rights, guaranteed by Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (the 'ECHR') and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (the 'Charter'), and elaborated in the Data Protection Directive 95/46/EC and related instruments.

[1] DPI technologies examine different layers (header and content) of data packets and, based on the findings, further process those packets. Resulting actions include packet routing, prioritisation, blocking etc. according to predefined policies. Examples of resulting actions are prioritisation or filtering of VoIP or P2P traffic by ISPs, or security specific measures when malware is found in the packets.

[2] See https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Traffic%20Management%20Investigation%20BEREC_2.pdf .

Postal address: rue Wiertz 60 - B-1047 Brussels
Offices: rue Montoyer 30
E-mail : edps@edps.europa.eu - Website: www.edps.europa.eu
Tel.: 02-283 19 00 - Fax : 02-283 19 50

Confidentiality is also protected in EU secondary legislation, namely by Article 5 of the ePrivacy Directive[3].

The importance of respecting privacy and data protection increases with the convergence of all communications on the Internet and the more and more central role it takes in everybody's life. Internet Service Providers could gain an unparalleled insight into their users' private life if they could freely access and process their communications for their own purposes.

The EDPS has already contributed to the debate on many occasions, in particular through the comments submitted on the Commission's public consultation on "The open Internet and net neutrality in Europe"[4] and the EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data.[5]

Yet we wish to take the opportunity of this public consultation to stress certain issues raised by the questions of the consultation so that the Commission can take the EDPS' considerations into account when developing future related policy actions.

II. General issue: Internet traffic management and personal data (question 9)

As stated in our Opinion on net neutrality, we support the concept of an open Internet. ISPs are entitled to develop traffic management measures, provided that they are fully respectful of privacy and data protection requirements.

The use of DPI techniques involves the processing by ISPs of considerable amounts of data relating to Internet users, many of which are considered to be personal data (e.g. IP addresses), confidential (e.g. the content of communications)[6], or even sensitive (e.g. information relating to health). In accordance with Article 7 of the Data Protection Directive 95/46/EC and Article 5 of the ePrivacy Directive, an appropriate legal ground must be found to justify the processing of personal data in the context of Internet traffic management.

Traffic management is performed by ISPs for many different purposes. Traditional purposes are network security and congestion management. Traffic inspection techniques are based on the analysis of the Internet protocols at different layers of the packet, mainly to read the source and destination IP addresses and the Internet protocols, which in most cases is sufficient for the purposes of congestion

[3] 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 (Directive on privacy and electronic communications), OJ L 201, 31.07.2002 p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

[4] EDPS comments on the Commission public consultation on "The open Internet and net neutrality in Europe", 6 October 2010, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Comments/2010/10-10-06_EC_Consultation_Open_Internet_EN.pdf .

[5] See EDPS Opinion on net neutrality, traffic management and the protection of privacy and personal data, 7 October 2011, available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-10-07_Net_neutrality_EN.pdf.

[6] See Article 29 Working Party Opinion on the concept of personal data, 20 June 2007, p.16-17, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

management and traffic limitation. As the EDPS explained in details in his Opinion on net neutrality[7], under the ePrivacy Directive ISPs may usually carry out this type of processing for purpose of conveying the communications, safeguarding the security of the communications service, or minimising congestion.

Over the years, new purposes have arisen like service specialisation and differentiation of levels of service, based or not on contracts with the customer, leading to Internet traffic inspection and filtering according to the specific service/application. More recent objectives involving comprehensive internet traffic inspection include behavioural analysis and profiling, mainly used for security purposes but also for commercial, copyright protection and other uses. These new purposes can be far more intrusive than the traditional ones from a privacy and data protection perspective, in particular when they may entail the monitoring of Internet subscribers' behaviour online[8]. As the EDPS described in his Opinion on net neutrality[9], some of these processing activities may go beyond the scope of what the law would allow. In particular, where these processing operations have not been explicitly foreseen under the ePrivacy Directive and/or are not fully respectful of other obligations incumbent upon ISPs, such as those set forth in Article 15 of the E-commerce Directive, it must be assessed carefully at least (i) whether each of these processing operations are necessary and proportionate to the aim pursued, and (ii) whether they have a sufficient legal basis under Article 7 of Directive 95/46/EC. In the absence of a ground in the law, they should be based on another legal ground, such as consent.

As a consequence, traffic management policies should be developed in full respect of fundamental rights and in compliance with the existing legal framework for electronic communications, E-commerce, and data protection.

III. Specific comments

a) DPI techniques and privacy risks (question 10a)

A detailed description of the issues raised by the use of deep packet inspection from a privacy and personal data protection perspective can be found in the EDPS Opinion on net neutrality[10]. Risks to privacy, data protection and communication confidentiality are very high due to the high intrusive feature of DPI, which scans the whole content of the IP packets to find out specific patterns against pre-defined criteria established in inspection policies.

The impact of these measures is furthermore increased due to the growing convergence of all kinds of communications through the Internet, including those containing sensitive personal data. Furthermore, traditional communications are now shifting to the Internet. Ubiquitous access is boosted by the growing offer of services for "smart" mobile devices. Further to adding traditional phone cell related location

[7] See further details in EDPS Opinion on net neutrality, pages 10-12.

[8] Measures that aim at the general monitoring of the Internet can only be done in accordance with the law (in particular Article 15 of the E-commerce Directive). This principle was recalled by the European Court of Justice of the EU in the case C-70/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Judgement of 24 November 2011.

[9] See EDPS Opinion, pages 10-14.

[10] See section V.4, p.17.

data to the usually processed information, the use of "smart" devices allows gathering further information from the sensors they incorporate, like more fine grained location data thanks to GPS antennas and high resolution cameras. In some cases (use of the same ISPs and even of the same physical gateway) all kinds of communication flow through the same access point, thus increasing the physical convergence of personal data relating to the same individual and to the other individuals with whom he communicates.

As a consequence, ISPs might gather large amounts of data related to the same individual that may ease comprehensive intelligence gathering and profiling. Furthermore, there could be a temptation to use unlawfully gathered personal data for commercial purposes, in particular for behavioural and targeted marketing. Experience has shown that the availability of new data collection and processing possibilities often creates interest in using the available data for new purposes, beyond what was originally intended, communicated to the individuals concerned and agreed by them. The setting up of comprehensive infrastructures for DPI in communications networks may trigger such interests, e.g. for economic or law enforcement reasons. Unless the infrastructure is equipped with the means to detect non-permitted use, it may be difficult to detect and prove the resulting infringements of privacy.

b) Traffic management and alternatives to DPI (question 10b)

Traditional traffic management techniques have used the packet header information fields to process packet flows. Some of the new Internet application/service types cannot any longer be identified just by inspecting the protocol related fields but bear their identity in the packet payload[11]. Sometimes this is done on purpose (standard TCP/UDP port change, tunnelling, etc.) to hamper an easy identification of the application. For more fine-grained control, the information is searched in the payload.

The EDPS believes that research on privacy-friendly alternatives to DPI should be encouraged. In this view, he wishes to underline specific points that should be taken into consideration to help develop privacy-friendly alternatives:

- The purpose limitation and proportionality principles should always be of guidance in exploring and adopting current and future traffic and communication management/processing techniques. The proportionality principle, as embedded in Article 6(c) of the Directive 95/46/EC, requires that the processing of personal data is 'not excessive in relation to the purposes for which they are collected'. As the EDPS noted in his Opinion, the principle of proportionality should serve as the guiding principle for the ISPs; it should promote the use of the least intrusive methods to inspect electronic communications and application of data protection safeguards, such as pseudo-anonymisation.[12]

- Communication protocols standardisation process has always aimed at setting the application/service information fields at the protocol level (in general, by

[11] For a basic introduction to the transmission of the information through the Internet and inspection techniques, see sections IV.1 and IV.2 of the Opinion, op.cit.

[12] See Opinion on net neutrality, traffic management and the protection of privacy and personal data, October 7, 2011, paragraphs 68-72, op.cit.

definition, at the application layer). The EDPS believes that this fundamental intent should be kept in the future and encourages efforts towards assessing the current adequacy of the Internet protocol stack with respect to the latest market needs.

- In many cases, services that might require specific traffic management practices can be identified by the IP addresses they use (e.g. search engines, video portals). The use of the IP address of the requested services as an indicator of the type of service should be pursued for service identification. This information could also be useful for better routing of the requested resources to the client.

- Research on methods allowing inferring the requested service/application type from some statistical features of the packets and packet stream should be encouraged.

- A fair bandwidth offer sized on what is defined in the contract between the ISP and the subscribers would limit the problem.

c) Communications inspection, security, and accountability measures

As explained by the EDPS in his Opinion[13], Article 4 of the ePrivacy Directive explicitly requires ISPs to take technical and organizational measures to guarantee a level of security appropriate to the risk presented.[14]

Considering, as described in section III.a) above, that scanning the packets payload is a high risk processing operation in terms of possible impact on privacy and data protection, the technical and organisational safeguards to be put in place should therefore be as strong and effective as to counter those risks, especially with regard to possible misuse of the data.

The mandatory "implementation of a security policy with respect to the processing of personal data", as provided for by the Article 4 of the ePrivacy Directive, should be the result of an adequate assessment of the risks for fundamental freedoms. It is worth noting that the Commission proposal for a General Data Protection Regulation proposal (hereinafter the proposed Regulation)[15], explicitly provides for "an evaluation of the risks"[16] with a view to establish the most appropriate measures.

[13] See section V.4, p.17, op.cit.

[14] Those measures, as a minimum requirement, will ensure *(i)* that personal data is only accessed by authorised personnel and for lawful purposes; *(ii)* protection of personal data from accidental or unlawful processing, and *(iii)* implementation of a security policy with respect to the processing of personal data. It also enables national competent authorities to perform audits on these measures and to issue recommendations about best practices concerning the level of security which those measures should achieve. In case of data breach, ISPs must notify it to the national data protection authority (DPA). In case personal data or privacy of subscribers is affected ISPs are obliged to notify them without undue delay of the incident, unless they can demonstrate that they have set up measures to protect the confidentiality of those data. As a preventive measure, ISPs need also to notify subscribers of particular risks of breach of the security of the network.

[15] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, of 25 January 2012, COM(2012)11 final, currently undergoing legislative process by the European Parliament and the Council.

[16] See Article 30. 2 of the draft Regulation.

Article 33 of the proposed Regulation requires that an impact assessment be carried out for certain processing operations presenting specific risks to privacy and data protection. In this perspective, the EDPS encourages a further assessment of which practices of deep packet inspection might require a mandatory data protection impact assessment.

The respect of privacy by default and privacy by design (as provided for in Art. 23 of the draft Regulation) should also guide ISPs in the design of their infrastructure and services. Privacy by design and by default has consequences on the offer of services to subscribers. For example ISPs should offer services where the processing/filtering of personal data is minimised. Privacy by default and by design principles should also be taken into account by companies providing solution for generic and specialised traffic management.

Furthermore, the use by ISPs of relevant privacy certification schemes and seals could increase the level of reasonable assurance of privacy-friendly processing and boost the respective market.

The EDPS believes that ISPs should demonstrate a high level of accountability (as provided for in Article 22 of the draft Regulation), not only towards competent authorities but also towards the data subjects.

Finally, the relevant national authorities, e.g. Data Protection Authorities, shall be able to audit the security measures, as provided for by Article 4 of the ePrivacy Directive.

d) Transparency and data subject's consent in traffic management (questions 10 and 11)

In view of the high risks that certain traffic management techniques entail for data subjects, the EDPS has consistently called for transparency from the ISP's side. The subscribers of the communication services are entitled to the adequate level of information as regards the business practices applied by the ISPs. This requirement of transparency actually extends to all users concerned by the communication. Consumers' informed choice is conditional and possible only if the service provider is transparent about his business practices.

The EDPS wishes to share the following considerations on possible ways to present their traffic management policies in a transparent way:

- In general, ISPs must provide their customers with appropriate information related to their traffic management policies. From a data protection perspective, appropriate information should encompass all the information required under Articles 10 and 11 of Directive 95/46/EC. Such information may be provided together with the contractual terms; it should however be clear and stand out of the typical contractual clauses.

- Furthermore, specific information should be provided in respect of traffic management policies that involve more intrusive processing for which consent needs to be sought (such as reading of certain content layers, profiling, etc). For

instance, it would be advisable that such information warns the subscriber about the intrusiveness that such processing entails from a privacy and data protection perspective, and that it indicates the possibility for the subscriber to withdraw his consent at any time.

- In order to collect valid consent to apply traffic management policies that involve more intrusive processing activities, ISPs must ensure that consent is based on an affirmative action from the data subject and is free, specific, and informed. Therefore, such consent cannot be collected by simply signing the general contractual offer, since such consent would not be considered to be specific enough. In this respect ISPs need to ascertain carefully which processing activities require consent, and they must ensure that they can respect any further choice to opt-out from such processing.

- ISPs bear a responsibility for informing customers about any update or changes to their traffic management policies. Where consent is needed for such changes or updates, ISPs should again seek a free, specific and informed indication of wishes from their subscribers. ISPs should reach out to their customers in the most appropriate manner to notify them about the changes, and to seek their individual consent where that is needed. Simply posting changes on an Internet home website would not constitute an appropriate notification of such changes.

Brussels, 15 October 2012