EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor

on net neutrality, traffic management and the protection of privacy and personal data

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular Articles 7 and 8 thereof,

Having regard to 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[1],

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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[2], and in particular Article 41(2) thereof,

Having regard to 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],

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. Background

1. On 19 April 2011, the Commission adopted a Communication on the open internet and net neutrality in Europe[4].

2. This Opinion can be seen as the reaction of the EDPS to this Communication and aims at contributing to the ongoing policy debate within the EU on net neutrality, especially on aspects related to data protection and privacy.

[1] OJ L 281/31, 23.11.95, pp. 31–50, the 'Data Protection Directive'.
[2] OJ L 8, 12.1.2001, p. 1, the 'Data Protection Regulation'.
[3] OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (see footnote 15), the 'ePrivacy Directive'.
[4] COM(2011) 222 final.

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

3. The Opinion builds on the answer[5] of the EDPS to the Commission's public consultation on The Open internet and net neutrality in Europe, which preceded the Commission's Communication. The EDPS has also taken note of the recent draft Council conclusions on net neutrality[6].

I.2. The concept of net neutrality

4. Net neutrality refers to an ongoing debate on whether Internet service providers ('ISPs[7]') should be allowed to limit, filter, or block Internet access or otherwise affect its performance. The concept of net neutrality builds on the view that information on the Internet should be transmitted impartially, without regard to content, destination or source, and that users should be able to decide what applications, services and hardware they want to use. This means that ISPs cannot, at their own choice, prioritise or slow down access to certain applications or services such as Peer to Peer ('P2P'), etc[8].

5. Filtering, blocking and inspecting network traffic raises important questions, often overlooked or sidelined, regarding the confidentiality of communications and the respect for the privacy of individuals and their personal data when they use the Internet. For instance, certain inspection techniques involve the monitoring of content of communications, websites visited, emails sent and received, the time when this takes place, etc, enabling filtering of communications.

6. By inspecting communications data, ISPs 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.

I.3. Focus and structure of the Opinion

7. The EDPS considers that a serious policy debate on net neutrality must address the confidentiality of communications as well as other privacy and data protection implications.

8. This Opinion contributes to this ongoing EU debate. Its goal is threefold:
   - It flags the relevance of privacy and data protection in the current discussions on net neutrality. More particularly, it highlights the need to respect the existing rules on confidentiality of communications. Only practices that respect such rules should be allowed.

---

[5] EDPS responded stressing the importance of taking into account data protection and privacy issues together with other existing rights and values. The response is 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.

[6] Available at http://register.consilium.europa.eu/pdf/en/11/st14/st14209.en11.pdf.

[7] This includes the provision of both fixed and mobile access to the Internet.

[8] Although the principle does apply to ISPs putting limits on the speed or amount of information a subscriber is able to send or receive through subscriptions with bandwidth or volume limits. Therefore, under a net neutrality principle ISPs would still be able to offer Internet access subscriptions limiting access based on criteria such as speed or volume as long as it does not require discriminating in favour or against particular content.

- Net neutrality relates to relatively new - technological - possibilities and there is little experience on how the legal framework applies. This Opinion therefore provides guidance on how ISPs must apply and respect the data protection legal framework if they engage in filtering, blocking and inspecting network traffic. This should be helpful for ISPs and also for authorities in charge of enforcing the framework.
- Within the scope of data protection and privacy, this Opinion identifies areas which call for special attention and which may require action at EU level. This is particularly important in the light of the ongoing debate at EU level and the policy measures that may be launched by the Commission in this context.

9. The EDPS is aware that net neutrality raises other issues, further described below, such as those related to access to information. These issues are only addressed to the extent that they are related to or have an impact on data protection and privacy.

10. The Opinion is structured as follows. Section II starts by providing a short overview of practices on filtering by ISPs. Section III outlines the EU legal framework on net neutrality. Section IV continues with a technical description followed by an assessment of the privacy implications, depending on the technique used. Section V analyses the practical details regarding the application of the current EU privacy and data protection framework. Building on the analysis, Section VI contains suggestions for further policy developments and identifies the areas where clarification and improvement of the legal framework might be needed. Section VII contains the conclusions.

II. NET NEUTRALITY AND TRAFFIC MANAGEMENT POLICIES

Increasing use of traffic management policies

11. Traditionally, ISPs have engaged in monitoring and influencing network traffic only in limited circumstances. For example, ISPs have applied inspection techniques and restricted information flows to preserve the security of the network, e.g. to fight viruses. Therefore, generally speaking, the Internet has grown while preserving a great degree of neutrality.

12. However, in recent years, some ISPs have shown an interest in inspecting network traffic in order to differentiate and apply different policies to it, for example, to block specific services or give preference access to others. This is sometimes referred to as 'traffic management policies'[9].

13. The reasons for ISPs to inspect and differentiate traffic are manifold. For example, traffic management policies may help ISPs to manage traffic during periods of high congestion, for example, by prioritising certain time-sensitive traffic, such as video streaming and downgrading other types of traffic which may be less time sensitive,

[9] See for example, OFCOM Report entitled 'Site blocking to reduce online copyright infringement', adopted on 27 May 2011, available at: http://www.culture.gov.uk/images/publications/Ofcom_Site-Blocking-_report_with_redactions_vs2.pdf: 'Some ISPs already deploy packet inspection systems in their network for traffic management and other purposes, so we assume that it can be deployed, albeit that this would involve a high level of complexity and cost for those not already running such services. It may be that in the short to medium term DPI could only be deployed by the larger ISPs given the capital investment required'.

such as P2P[10]. Furthermore, traffic management may be a means for ISPs to obtain a potential revenue stream, which could originate from different sources. On the one hand, ISPs could charge fees to content service providers, for example, those whose services require using higher bandwidth, in exchange of giving them priority (and thus speed). This would mean that accessing a certain service, for example, a service providing videos on demand, would be faster than accessing another similar service which has not signed up to high speed transmission. Revenues could also be obtained from subscribers interested in paying higher (or lower) fees for certain types of differentiated subscriptions. For example, a subscription without access to P2P could be cheaper than one giving unlimited access.

14. In addition to the ISP's own reasons for the use of traffic management policies, other parties may also have an interest in ISP's using traffic management policies. If ISPs manage their networks and engage in inspection of content which goes through their facilities, they are likely to increase their capacity to detect alleged unlawful usage, e.g. breach of copyright or pornographic use.

Other interests at stake, including data protection and privacy

15. This trend has triggered a debate on the legitimacy of this type of practices and more particularly whether specific net neutrality obligations should be further developed by law.

16. Increasing use by ISPs of traffic management policies could possibly limit access to information. If this behaviour became common practice and it was not possible (or highly expensive) for users to have access to the full Internet as we know it, this would jeopardise access to information and user's ability to send and receive the content they want using the applications or services of their choice. A legally mandatory principle on net neutrality may avoid this problem.

17. This brings the EDPS to the implications for data protection and privacy when ISPs engage in traffic management. More particularly:

- When ISPs process traffic data with the sole purpose of routing the information flow from the sender to the receiver, they generally carry out limited personal data processing[11]. In the same way as the postal service processes the information included on the envelope of a letter, the ISP processes the information needed to route the communication towards the recipient. This does not conflict with the legal requirements of data protection, privacy and confidentiality of communications.
- However, when ISPs inspect communication data in order to differentiate each communication flow and to apply specific policies, which may be unfavourable to individuals, the implications are more significant. Depending on the circumstances of each case and on the type of analysis performed, the processing may be highly intrusive for an individual's privacy

10 The quality of real-time applications such as video streaming is, among other things, dependent on latency, i.e., delay due for example to network congestion.

11 This excludes operations aimed at increasing the security of the network and detecting harmful traffic and also operations required for billing and interconnection. It also excludes obligations that derive from the Data Retention Directive, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ 2006, L 105/54 ('Data Retention Directive').

and personal data. This is more obvious where management policies reveal the content of individuals' Internet communications, including emails sent and received, websites visited, files downloaded or uploaded, etc.

III. OVERVIEW OF THE EU LEGAL FRAMEWORK ON NET NEUTRALITY AND FURTHER POLICY DEVELOPMENTS

III.1. The legal framework in a nutshell

18. Until 2009, EU legislative instruments did not contain provisions explicitly prohibiting ISPs from engaging in filtering or blocking or charging extra costs to subscribers for access to services. At the same time, they did not contain provisions explicitly recognising this practice. The situation was, to some extent, one of uncertainty.

19. The 2009 Telecom package changed this by including provisions favouring the openness of the Internet. For example, Article 8(4) on a common regulatory framework for electronic communications networks and services ('Framework Directive') establishes an obligation on regulatory authorities to promote the ability of end users to access content, applications or services of their choice[12]. This provision applies to the network as a whole, not at the level of individual providers. Recent draft Council conclusions also highlighted the need to maintain the openness of the Internet [13].

20. The Universal Service Directive[14] contains more concrete obligations. Articles 20 and 21 set forth transparency requirements regarding limitations on access to and/or use of services and applications. It also requires minimum service quality levels.

21. For ISP practices entailing the inspection of individuals' communications, Recital 28 of the Directive amending the Universal Service and ePrivacy Directives[15] highlights that 'depending on the technology used and the type of

---

[12] Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services, as amended by Directive 2009/140/EC and Regulation 544/2009, OJ 337, 18.12.2009, p. 37.

[13] See point 3(e), where Council recognises: 'The need to maintain the openness of Internet while ensuring that it can continue to provide high-quality services in a framework that promotes and respects fundamental rights such as freedom of expression and freedom to conduct business' and 8(d), inviting Member States to 'Promote the open and neutral character of the Internet as their policy objective'.

[14] Directive 2002/22/EC as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. OJ L 337/11, 18.12.2009. Compare also Article 1(3), stating that the Directive neither mandates nor prohibits ISPs from limiting end-users' access to, and/or use of, services and applications, where allowed under national law and in conformity with Community law, but requires them to inform about any such conditions.

[15] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws. OJ L 337/11, 18.12.2009.

limitation, such limitation may require user consent under the ePrivacy Directive'. Thus, Recital 28 recalls the need for consent pursuant to Article 5(1) of the ePrivacy Directive for any limitations based on monitoring of communications. Section IV below further analyses the application of Article 5(1) and the overall data protection and privacy legal framework.

22. Finally, Article 22(3) of the Universal Service Directive now empowers national regulatory authorities to impose, if necessary, minimum quality of service requirements on ISPs in order to prevent the degradation of services and the hindering or slowing down of traffic over public networks.

23. The above means that at the EU level there is a broad aspiration to an open Internet (see Article 8(4) of the Framework Directive). However, this policy objective, which applies to the network as a whole, is not directly linked to prohibitions or obligations on individual ISPs. In other words, an ISP could engage in traffic management policies, which may exclude access to certain applications, provided that end-users are fully informed, and have expressed their consent freely, specifically and unambiguously.

24. The situation may differ depending on Member States. In some Member States ISPs can, under specific conditions, engage in traffic management policies, for example, to block applications such as VoIP (as part of a cheaper Internet subscription), provided that individuals have given their free, specific and unambiguous, informed consent. Other Member States have chosen to strengthen the principle of net neutrality. For instance, in July 2011 the Dutch Parliament passed a law generally prohibiting providers from hindering or slowing down applications or services on the internet (such as VoIP), unless necessary to minimise the effects of congestion, for integrity or security reasons, to fight spam or in accordance with a court order.[16]

III.2. The Communication on Net Neutrality

25. In its Communication on net neutrality[17], the European Commission concluded that the situation on net neutrality is one that requires monitoring and further analysis. Its policy has been dubbed as 'wait and see', before considering further regulatory steps.

26. The Commission's Communication recognised that any measure and further regulatory steps would be subject to an in-depth assessment of data protection and privacy aspects. The draft Council conclusions also note the data protection and privacy issues at stake.[18]

27. The question to be assessed from a data protection and privacy perspective is whether a wait and see policy is sufficient. While the data protection and privacy framework does, at the present time, foresee some safeguards especially through

---

[16] The original Dutch amendment can be found at: https//zoek.officielebekendmakingen.nl/kst-32549-A.html The reasons reported by the press for such a policy option did not refer to data protection and privacy considerations but rather to reasons related to ensuring that users are not deprived of or are offered limited access to information. So it seems that issues relating to access to information motivated this amendment.

[17] See footnote 4.

[18] See point 4(e), where Council notes: 'The existence of some concerns, mainly emerging from consumers and data protection authorities, in regard to personal data protection'.

the principle of confidentiality of communications, it appears necessary to monitor closely the level of compliance and issue guidance on several aspects that are not particularly clear. In addition, some thoughts should be put forward as to how the framework could be clarified and further improved, in the light of technological developments. If the monitoring reveals that the market is evolving towards massive, real-time inspection of communications and issues related to complying with the framework, legislative measures will be necessary. Concrete suggestions will be made in that respect in Section VI.

IV. TECHNICAL BACKGROUND AND RELATED PRIVACY AND DATA PROTECTION IMPLICATIONS

28. Before going more deeply into the subject, it is important to have a better view of the inspection techniques that may be used by ISPs to engage in traffic management and how this may impact the principle of net neutrality. The privacy and data protection implications derived from such techniques vary substantially depending on which technique/s is or are used. This technical background is necessary to understand and apply properly the legal data protection framework described in Section V. However, it should be noted that this is a constantly changing and complex area. The description below therefore is not intended to be exhaustive and fully up-to-date, but only to provide the technical information that is indispensable for understanding the legal reasoning.

IV.1. Transmission of information through the Internet: the basics

29. When a user transmits a communication via Internet, the information transmitted is divided into packets. These packets are transmitted across the Internet from the sender to the recipient. Each packet will include, among others, information about the source and the destination. In addition, ISPs might enclose these packets into additional layers and protocols[19], which will be used to manage the different traffic flows within the ISP network.

30. To refer back to the analogy of the postal letter, using a network transmission protocol is equivalent to including the content of a postal letter into an envelope with a destination address to be read by the postal service and then having the postal service deliver it. The postal service may use additional protocols in its internal transits to manage all the envelopes to be transmitted, the goal being that each envelope reaches its destination as originally drafted by the sender. Using this analogy, each packet has two parts, the *IP payload* that includes the content of the communication and will be the equivalent to the letter. It contains information addressed only to the recipient. The second part of the packet is the *IP header* that includes, among others, the address of the recipient and the sender and will be the equivalent to the envelope. The IP header allows the ISPs and other intermediaries to route the payload from its source address to its destination address.

31. ISPs and other intermediaries ensure that IP packets travel across the network through nodes that read the IP header information, check it versus routing tables, and then forward them towards the next node in the path to the destination. This

[19] As further described in Section IV.2, such protocols code the information being transmitted end-to-end in an agreed way so that the parties involved in the communication can understand each other, such as HTTP, FTP, etc.

process is done across the network using a 'best effort memoryless' approach since all the packets arriving to a node are treated in a neutral way. When they have been forwarded to the next node, there is no need to retain further information in the router[20].

IV.2. Inspection techniques

32. As illustrated above, ISPs read IP headers for the purpose of routing them towards their destination. However, as outlined above, the analysis of traffic (involving IP headers and IP payloads) can be performed for other purposes and with different types of technologies. New trends may include for instance slowing down certain applications being used by users, such as P2P, or alternatively, enhancing traffic speed for certain services like video-on-demand services for premium subscribers. While all inspection techniques *technically* perform packet inspection, they involve different levels of intrusiveness. There are two main categories of inspection techniques. One is based on just the IP header, the other also on the IP payload.

- *Based on the IP header information.* The inspection of an IP packet header reveals some fields that may allow ISPs to apply a number of specific policies to manage the traffic. These techniques based only on inspection of IP headers process data which, in principle, is meant for routing information, for a different purpose (i.e. differentiating traffic). Looking at the source IP address, the ISP can link it to a concrete subscriber and apply some specific policies, for instance routing the packet through a faster or a slower link. Looking at the destination IP address, the ISP can also apply specific policies, for instance blocking or filtering access to certain websites.

- *Based on a deeper inspection.* Deep packet inspection enables the ISP to access information addressed to the recipient of the communication only. Going back to the postal service example, this approach is equivalent to opening the envelope and reading the letter inside to perform an analysis of the content of the communication (encapsulated inside the IP packets) in order to apply a specific network policy. There are different ways of carrying out the inspection, each presenting different threats to the data subject.

  - *Deep packet inspection based on the analysis of protocols and on statistical records.* In addition to the IP protocol, which is meant to enable the data to be transmitted across the Internet, there are additional protocols that code the information being transmitted in an agreed way (transport, session, presentation and application, etc.). The goal of these protocols is to ensure that the parties involved in the communication can understand each other. For instance, there are some protocols that are associated with web browsing[21], others are for file transfer[22], etc. Therefore inspection techniques based on the inspection of protocols and combined with statistical analysis aim at looking for specific patterns or

[20] Nevertheless, Internet network equipment uses routing protocols that will log activity, process traffic statistics, and exchange information with other network equipment in order to route IP packets using the most efficient path. For instance, when a link is congested or broken, and a router receives this information, it will update its routing table with some alternative not using that link. It is also worth noting the collection and processing that in some cases may be done for billing purposes or even in accordance with the requirements of the Data Retention Directive.

[21] HTTP - Hypertext transfer protocol - or HTML - Hypertext Markup Language.

[22] FTP - File transfer protocol.

fingerprints that determine which protocols are present[23]. These inspection techniques enable the ISPs to understand the type of communication (email, web browsing, uploading files) and, in some cases, to identify the specific service or application used, such as the case of some VoIP communications where the protocols used are very specific to a concrete vendor or service provider. The knowledge of the type of communication by itself can allow ISPs to apply concrete traffic management policies. For example, to block web traffic. It may also be the first step in allowing the ISP to perform further analyses that might require full access to the metadata and content of the communication.

- *Deep packet inspection based on the analysis of the content of the communication.* Finally, it is also possible to inspect the metadata[24] and the content of a communication itself. This technique consists in the interception of all the IP packets that are part of the original communication flow so that the original content of the communication can be reconstructed in full and analysed. For example, to detect harmful or illegal content like viruses, child pornography, etc, it is necessary to reconstruct the content itself so that it can be analysed. It is to be noted that sometimes the communication can be explicitly encrypted end-to-end by the parties involved and this practice will impede ISPs to perform analysis of the content of the communication.

IV.3. Privacy and data protection implications

33. Inspection techniques based on IP headers and more particularly those based on packet inspection involve the monitoring and filtering of these data and have serious implications in terms of privacy and data protection. They can also be in conflict with the right to confidentiality of communications.

34. Looking into individuals' communications has, in itself, serious privacy and data protection implications. Yet, the problem is broader since, depending on the effects pursued with the monitoring and interception, the privacy implications may further increase. Indeed, it is not the same to merely inspect communications, for example, to ensure that the system works well, and to inspect communications to apply policies which may have an impact on individuals. When traffic and selection policies may seek to avoid network congestion only, there will usually be no major implications for individual's privacy. However, traffic management policies may seek to block some content information, or influence the communication for instance through behavioural advertising. In those cases the effects are more intrusive. The concern becomes more critical if one realises that this type of information would be collected not for a small group of individuals but rather on a generalised basis, for all ISP customers[25]. If all ISPs embrace filtering techniques,

---

[23] There are different ways of identifying the protocols used. For example, it is possible to search in specific fields in inner protocols, e.g. to identify ports used to establish the communication. A statistical characterization of a communication flow can also be inferred from the analysis of some specific fields, correlation of the protocols used simultaneously between two IP addresses.

[24] Each protocol has some specific fields in its header that provide additional informal information about the communication being transmitted. Therefore the content of those fields can be referred to as the metadata of the communication. An example of these fields can be the port number used, where, for instance if it is number 80, it is quite likely that the type of communication is web browsing.

[25] Of course, tracking capabilities are not exclusive to ISPs. Instead, ad. network providers are also capable, through the use of third party cookies to track users across websites. See for example a recent

this could lead to a generalised monitoring of Internet usage. Furthermore, if one focuses on the type of information being processed, the risks to privacy are obviously high, as much of the information being collected is likely to be very sensitive and, after collection, is available to ISPs and to those who would seek information from them. Furthermore, the information might also be very valuable in commercial terms. In itself, this represents a high risk of function creep where the initial purposes could easily evolve into commercial or other exploitation of the information collected.

35. The correct application of monitoring and inspection and filtering techniques must be done in conformity with the applicable data protection and privacy safeguards, which lay down limits as to what can be done and under which circumstances. Next follows an overview of the applicable safeguards under the current EU data protection and privacy legal framework.

V. APPLICATION OF THE EU PRIVACY AND DATA PROTECTION LEGAL FRAMEWORK

36. The EU data protection framework is technologically neutral; as such, it does not regulate specific inspection techniques as those described above. The ePrivacy Directive regulates privacy in the provision of electronic communication services in public networks (typically Internet access and telephony)[26] and the Data Protection Directive regulates data processing in general. Taken as a whole this legal framework sets out different obligations that apply to ISPs that process and monitor traffic and communications data.

V.1. Legal grounds to process traffic and content data

37. Under data protection legislation, the processing of personal data, such as in this case the processing of traffic and communication data, requires an adequate legal ground. In addition to this general requirement, specific requirements may apply in certain cases.

38. In this case, the type of personal data that are processed by ISPs refers to the traffic data and content of communications. The content of communications and the traffic data are both protected by the right to confidentiality of correspondence, which is guaranteed by Article 8 ECHR and Article 7 and 8 of the Charter. More particularly, Article 5(1) of the ePrivacy Directive, entitled 'confidentiality of communications' requires Member States to ensure the confidentiality of

---

academic article showing that Google has a presence on 97 of the top 100 websites, which means that Google can track users who have not opted out of third party cookies as they browse these popular websites. See: Ayenson, Mika, Wambach, Dietrich James, Soltani, Ashkan, Good, Nathan and Hoofnagle, Chris Jay, Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning (July 29, 2011). Available at SSRN: http://ssrn.com/abstract=1898390. The tracking of users through third party cookies has been addressed by the Article 29 Working Party. See Opinion 2/2010 on online behavioural advertising, adopted on 22 June 2010 (WP 171).

[26] Article 1.2 of the ePrivacy Directive reads: 'In the electronic communications sector, Directive 95/46/EC applies in particular to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of this Directive, including the obligations on the controller and the rights of individuals'. Also, Recital 17 is relevant in relation to data subject consent: 'For the purposes of this Directive, consent of a user or subscriber, regardless of whether the latter is a natural or a legal person, should have the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC'.

communications and the related traffic data by means of a public communications network and publicly available electronic communications services. At the same time, Article 5(1) of the ePrivacy Directive foresees that the processing of traffic and content data by ISPs may be allowed, in certain circumstances, with the consent of the users. This is done by setting forth a prohibition to the '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 is further developed below.

39. In addition to the consent of users concerned, the ePrivacy Directive foresees other grounds that may legitimise ISPs' processing of traffic and communication data. The relevant legal grounds for processing in this case are *(i)* delivering the service; *(ii)* safeguarding the security of the service, and *(iii)* minimizing congestion. Other possible grounds to legitimise management policies based on traffic or communication data are discussed below under *(iv)*.

(i) Legal grounds for delivering the service

40. As illustrated in Section IV, ISPs process the information on IP headers for purposes consisting in routing each IP packet towards its destination. Article 6(1) and Article 6(2) of the ePrivacy Directive allow processing of traffic data for the purposes of conveyance of a communication. Thus, ISPs may process the information that is necessary for the delivery of the service.

(ii) Legal grounds for safeguarding the security of the service

41. Pursuant to Article 4 of the ePrivacy Directive, an ISP is under a general obligation to take appropriate measures to safeguard security of its services. The practice of filtering viruses may involve the processing of IP headers and IP payload. Taking into account that Article 4 of the ePrivacy Directive requires ISPs to ensure the security of the network, this provision legitimises inspection techniques based on IP headers and content that aim strictly to achieve such purpose. In practice, this means that, within the limits set forth by the proportionality principle (see Section V.3), ISPs may engage in monitoring and filtering of communications data to fight viruses and overall ensure the security of the network.[27]

(iii) Legal grounds for minimising the effects of congestion

42. The *rationale* for this legal ground is to be found in Recital 22 to the ePrivacy Directive, explaining the Article 5(1) prohibition on storage of communications. This does not prohibit any automatic, intermediate and transient storage in so far as it takes place for the sole purpose of carrying out the transmission and does not last longer than necessary for the transmission and traffic management purposes, and the confidentiality of the communications remains guaranteed.

43. If there is a congestion, the question arises whether ISPs may consider randomly dropping or delaying traffic or rather slowing communications that are not time-

[27] Article 29 Working Party's Opinion 2/2006 on privacy issues related to the provision of email screening services, adopted on 21 February 2006 (WP 118). In this Opinion the Working Party considers that using filters for the purpose of Article 4 can be compatible with Article 5 of the ePrivacy Directive.

sensitive, e.g. P2P or email traffic, enabling, for example, voice traffic to pass at acceptable quality.

44. Given the overall societal interest of guaranteeing a usable communications network, ISPs may argue that prioritising or throttling traffic to address congestion is a legitimate measure which is necessary to deliver an adequate service. This means that in these cases and for this purpose, there would be a general legal ground for processing personal data and specific consent by users would not be necessary.

45. At the same time, the ability to interfere in this way is not unrestricted. If ISPs need to inspect communications, from the perspective of confidentiality, and applying strictly the proportionality principle, they must use the least intrusive method available to achieve the purpose (avoiding deep packet inspection), and they must only apply it for as long as necessary to resolve the congestion.

(iv) Legal grounds for processing data for other purposes

46. ISPs may also want to inspect traffic and content data for other purposes, for example offering targeted subscriptions (e.g. a subscription that limits access to P2P or a subscription that increases speed for certain applications). Inspection and further use of traffic and communication data for purposes other than delivering the service or ensuring its security and lack of congestion is only allowed under strict conditions, in compliance with the legal framework.

47. The legal framework is mainly Article 5(1) of the ePrivacy Directive which requires consent from users concerned to listen, tap, store or engage in other kinds of interception or surveillance of communications and the related traffic data. In practice this means that consent of users involved in a communication is necessary to legitimise the processing of both traffic and communications data pursuant to Article 5(1).

48. As explained above, the application of inspection and filtering techniques is either based on IP headers, which constitute traffic data, or based on deep packet inspection which also entails IP payloads and constitute communication data. Therefore, in principle, the application of such techniques for purposes other than the conveyance of the service or security would be forbidden unless a legitimate ground allows for the processing, such as consent (Article 5(1)). An example where Article 5(1) would apply is when an ISP decides to offer customers a reduced rate for Internet access in return for receiving behavioural advertising, using deep packet inspection, and thus communication data, in order to do so. Real, specific and informed consent is therefore necessary according to Article 5(1).

49. Furthermore, Article 6 of the ePrivacy Directive entitled 'traffic data' provides certain rules applying specifically to traffic data. More particularly it foresees the possibility for ISPs to process traffic data based on users' consent to receive value added services[28]. This provision specifies the consent requirement foreseen in Article 5(1) when traffic data are at stake.

[28] Recital 18 of the Directive contains a list exemplifying value added services. Whether services to which traffic management policies apply could be interpreted as part of the list is not clear. Traffic management policies aiming at prioritising certain content could be understood as providing a quality of the service. For example, traffic management that entails merely the processing of IP headers and has as its objective

50. In practice, it may not always be easy to ascertain, for example, in which cases consent is necessary, and in which cases the security of the network may legitimise the processing, particularly if the purposes of the inspection techniques are twofold (for instance avoiding congestion and providing added value services). It should be emphasised that consent cannot be considered as an easy and systemic gateway to compliance with data protection principles.

51. There is little experience on the application of the framework and more particularly on the various aspects that have been outlined above. This is an area where further guidance is essential, as further developed in Section VI. Furthermore, there are additional, relevant aspects related to obtaining consent that also require special consideration. These are described below.

V. 2. Issues related to providing informed consent as a legal ground

52. The consent required under Articles 5 and 6 of the ePrivacy Directive has the same meaning as the data subject's consent as defined and further specified in Directive 95/46/EC.[29] According to Article 2(h) of the Data Protection Directive, 'the data subject's consent' shall mean '*any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed*'. Recently, the role of consent and the requirements for it to be valid have been addressed by the Article 29 Working Party in its Opinion 15/2011 on consent[30].

53. ISPs requiring consent to engage in inspection and filtering of traffic and content data must therefore ensure that consent is free and specified, and it must be a fully 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 ' Below follow some practical examples of what it means in this context for consent to be free, specific and informed.

Consent: Free, specific and informed indication of wishes

54. *Free consent.* Users should not have to suffer constraints linking consent to the Internet subscription they want to sign up to.

55. Individuals' consent would not be freely given if they had to consent to the monitoring of their communication data in order to get access to a communication service. This would be even more true if *all* providers in a given market were to engage in traffic management for purposes that went beyond security of the network. The only option left would be not to subscribe to an Internet service at all. Given that the Internet has become an essential tool both for work and for leisure purposes, not subscribing to an Internet service does not constitute a valid

---

to offer premium-priced gaming services, where users' personal gaming traffic is prioritised through the network could be seen as a value added service. On the other hand, it is far from clear whether traffic management to throttle certain types of traffic, for example to downgrade P2P traffic could be deemed as such.

[29] See Recital 17 and Article 2(f) of the ePrivacy Directive.

[30] Adopted on 13 July 2011 (WP 187).

alternative. The result would be that the individuals would have no real choice, i.e. they would not be able to freely give consent[31].

56. The EDPS considers that there is a clear need for the Commission and national authorities to monitor the market, particularly to ascertain whether this scenario - i.e. providers linking telecommunication services to communication monitoring - becomes mainstream. Providers should offer alternative services, including an Internet subscription not subject to traffic management, without imposing higher costs to individuals.

57. *Specific consent.* The need for consent to be specific requires, in this case, that ISPs seek consent for the monitoring of traffic and communications data in a clear and distinctive way. According to the Article 29 Working Party, '... to be specific, consent must be intelligible: it should refer clearly and precisely to the scope and the consequences of the data processing. It cannot apply to an open-ended set of processing activities. This means in other words that the context in which consent applies is limited. ' Specific consent is not likely to be obtained if the consent for the inspection of traffic and communications data is 'bundled' with the overall consent to subscribe for the service. Instead, specificity calls for the use of targeted means to obtain consent, such as a specific consent form or a separate box clearly dedicated to the purpose of monitoring (rather than inserting the information in the general conditions of the contract and requiring signature of the contract as it stand).

58. *Informed consent.* For consent to be valid it must be informed. The need to provide adequate prior information derives not only from the ePrivacy and Data Protection Directives but also from Articles 20 and 21 of the Universal Service Directive, as amended by Directive 2009/136[32]. The need for information and consent was expressly confirmed in Recital 28 of Directive 2009/136: '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 require user consent under Directive 2002/58/EC '

59. Given the complexity of these monitoring techniques, giving meaningful prior information is one of the main challenges to obtain valid consent. Consumers should be informed in a way that they are able to understand the information that is being processed, how it is being used and the impact on the user experience and the level of privacy invasion related to the techniques.

60. This means not only that the information itself must be clear and understandable to average users, but also that the information is given directly to individuals in a conspicuous way so that they cannot overlook it.

---

[31] A similar case is PNR where it was discussed whether the consent of passengers to transfer the booking details to the US authorities was valid. The Working Party considered that passengers' consent cannot be given freely as the airlines are obliged to send the data before the flight departure, and passengers therefore have no real choice if they wish to fly; Opinion 6/2002 of the Article 29 Working Party on transmission of passenger manifest information and other data from airlines to the United States.

[32] 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 (see footnote 15).

61. *Indication of wishes.* 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. This also confirms the need to use dedicated means to obtain consent enabling the ISP to inspect traffic and communications data in the context of applying traffic management policies. In its recent opinion on consent, the Article 29 Working Party stressed the need for granularity in obtaining consent with regard to the different elements that constitute the data processing.

62. One could argue that if the parties involved in a communication do not want ISPs to intercept it in order to apply traffic management policies, they can always encrypt the communication. This approach can be considered as helpful in practical terms, however it requires some effort and technical knowledge and it cannot be deemed similar to a free, specific and informed consent. Also, the use of encryption techniques do not keep a communication fully confidential since the ISP at least will be able to access the IP header information in order to route the communication and it also will be in a position to apply statistical analysis.

63. According to Article 5(1) of the ePrivacy Directive, consent must be obtained from the users concerned. In many cases, the user will be the same person as the subscriber, which allows consent at the moment of subscription of the telecommunication service. In other cases, including those where more than one person may be involved, consent of the users concerned will need to be obtained separately. This may raise practical issues as developed below.

Consent of all the users concerned

64. Article 5(1) provides for user consent to legitimise the processing. Consent must be obtained from *all users* involved in a communication. The *rationale* behind this is that a communication usually concerns at least two individuals (the sender and the recipient). For example, if an ISP scans IP payloads which refer to an email, they are inspecting information that relates to both the sender and the receiver of the email.

65. When monitoring and intercepting traffic and communications (for example, some web traffic), it may suffice for ISPs to obtain the consent of the user, that is, the subscriber. This is because the other party to the communication, in this case, a website visited, may not be considered as a 'user concerned'[33]. However, the situation may be more complex when such monitoring involves inspecting the content of emails and thus, personal information of the email sender and recipient, who may not both have a contractual relationship with the same ISP. Indeed, in these cases, the ISP would be processing personal data (name, email address and potentially sensitive content data) of non-customers. From a practical perspective obtaining consent from such individuals may be more difficult, as it should be done on a case-by-case basis rather than at the occasion of the conclusion of the telecommunication service. Nor would it be realistic to assume that the subscriber's consent was also given on behalf of other users, as may often be the case in private households.

[33] Notwithstanding those cases where the web traffic involves the transfer of personal information such as, for example, pictures of identifiable natural persons posted on a website. The processing of such information requires a legal basis, but would not be covered by Article 5(1) as those persons would not be 'users concerned'.

66. In this context, the EDPS considers that ISPs should abide by existing legal requirements and implement policies which do not involve the monitoring and inspection of information. This is all the more essential with regard to communication services which involve third parties who are not able to consent to the monitoring, particularly with regard to emails sent and received (this does not apply when the purpose is based on security considerations).

67. At the same time, it should be noted that national law implementing Article 5(1) of the ePrivacy Directive may not always be satisfactory on this point, and that in general there seems rather to be a need for better guidance as to the requirements of the ePrivacy Directive in this context. The EDPS therefore invites the Commission to be more active in this respect and take an initiative which might benefit from the input from supervisory authorities assembled in the Article 29 Working Party and from other stakeholders. If necessary, a case should be brought before the Court of Justice in order to create full clarity about the meaning and the consequences of Article 5(1).

V.3. Proportionality - data minimisation principle

68. Article 6(c) of the Data Protection Directive lays down the proportionality principle[34], which applies to ISPs, as they are data controllers in the meaning of this directive, when they engage in monitoring and filtering.

69. Pursuant to that principle, personal data may be processed only insofar as they are 'adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed'. The application of this principle entails the need to make an assessment as to whether the means employed for the data processing and the types of personal data used are suitable and reasonably likely to achieve their objectives. If the conclusion is that more data is collected than necessary, then, the principle is not met.

70. The conformity with the proportionality principle of certain types of inspection technique must be assessed on a case by case basis. It is not possible to reach conclusions *in abstracto*. However, it is possible to point at various concrete aspects that should be evaluated in assessing compliance with the proportionality principle.

71. *The amount of information processed.* Surveillance of communications of ISP customers at the deepest possible levels will in most of the cases be excessive and illegal. The fact that this may be done by means that are not apparent to individuals and that it may be difficult for them to understand what is happening increases the impact on their privacy. ISPs should assess which less intrusive means may be available to achieve the result required. For example, can monitoring of IP headers achieve the result required, in place of engaging in deep packet inspection? Even when using deep packet inspection, the identification of only certain protocols may deliver the necessary information. The application of data protection safeguards, including pseudo-anonymization, may also be relevant. The outcome of the assessment must confirm that the data processing is proportional.

[34] As outlined above, the Data Protection Directive applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the ePrivacy Directive.

72. *The effects of processing (directly linked to the purposes).* Proportionality may be lacking in cases where ISPs use traffic management policies excluding access to certain services without allowing a fair share of the resulting benefit to users in return.

73. It is important to recall that the proportionality principle continues to apply even if other mandatory legal requirements have been satisfied, including if an ISP has, for example, obtained consent from individuals to engage in content monitoring. This means that the data processing carried out through content monitoring may still be illegal if it violates the underlying fundamental principle of proportionality.

V.4. Security and organizational measures

74. Article 4 of the ePrivacy Directive explicitly requires ISPs to take technical and organizational measures to 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.

75. In addition, pursuant to Article 4(3) and (2) of the ePrivacy Directive, ISPs are also obliged to notify respectively competent national authorities in the event of a data breach, as well as the individuals affected in case that the disclosure can have adverse consequences for them.

76. Processing personal information included in communications with the goal of applying traffic management policies can give ISPs access to data that is even more sensitive that traffic data.

77. Therefore, the security policies developed by ISPs should incorporate specific safeguards to ensure that the measures taken are adequate to these risks. At the same time, national competent authorities auditing these measures should be particularly demanding. Finally, it should be ensured that effective notification procedures are put in place to inform data subjects whose information has been compromised and who may thus be affected negatively.

VI. SUGGESTIONS FOR POLICY AND LEGISLATIVE MEASURES

78. Inspection techniques based on traffic data and inspection of IP payloads, i.e. the content of communications, may reveal users' Internet activity: websites visited and activities on those sites, use of P2P applications, files downloaded, emails sent and received, from whom, on what subject and in which terms, etc. ISPs may want to use this information to prioritise some communications, such as video on demand, over others. They may want to use it to identify viruses, or to build profiles in order to serve behavioural advertising. These actions interfere with the right to the confidentiality of communications.

79. Depending on the techniques used and on the specifics of the case, the privacy implications will increase. The deeper the interception and analysis of the information collected, the greater the conflict with the principle of confidentiality of communications. The purposes for which the monitoring takes place and the data protection safeguards that have been applied are also key elements to

determine the degree of intrusion into the privacy and personal data of individuals. Blocking and monitoring for purposes of fighting malware, with strict limitations on the retention and use of the data inspected, cannot be compared to situations where the information is logged to build individual profiles to serve behavioural ads.

80. In principle, the EDPS considers that the existing EU privacy and data protection framework, if properly interpreted, applied and enforced, would be appropriate to guarantee that the right to confidentiality is upheld and overall that the protection of the privacy and data protection of individuals is not jeopardised[35]. ISPs should not use such mechanisms unless they have properly applied the legal framework. More particularly, the relevant elements of the framework that ISPs should consider and respect include the following:

- ISPs can apply traffic management policies intending to provide security of the service, delivering the service, including limiting congestion, pursuant to Article 4 and 6 of the ePrivacy Directive.

- ISPs need another specific legal ground, and possibly users' consent, to apply traffic management policies which entail processing of traffic and/or communication data for purposes other than the above. For example, users' informed consent is necessary to monitor and filter the communications of individuals for the purposes of limiting (or allowing) access to certain applications and services such as P2P or VoIP.

- Consent must be free, explicit and informed. It should be indicated through an affirmative action. These requirements put strong emphasis on the need to step up the efforts to ensure that individuals are properly informed, in a way that is direct, understandable and specific so that they can assess the effects of the practices and ultimately make an informed decision. Given the complexity of these techniques, giving meaningful prior information to users is one of the main challenges to obtain valid consent. Besides, there should be no detrimental consequences (including financial costs) towards users who do not consent to any monitoring.

- The proportionality principle plays a crucial role when ISPs engage in traffic management policies, whatever the legal ground for processing and the purpose: delivering the service, avoiding congestion or providing targeted subscriptions with or without access to certain services and applications. This principle limits ISPs ability to engage in monitoring of the content of individual's communications that entail processing of excessive information or accruing benefits for ISPs only. What can logistically be performed by ISPs will depend on the level of intrusion of the techniques, the results required (for which they may accrue benefits) and the specific privacy and data protection safeguards applied. Prior to deploying inspection techniques, ISPs must engage in an assessment of whether these comply with the proportionality principle.

[35] This is without prejudice to the need for changes in the law based on other considerations, particularly in the context of the general review of the EU legal framework for data protection, with a view to making it more effective in the light of new technologies and globalisation.

81. While currently the legal framework includes relevant conditions and safeguards, there is a need to pay particular attention as to whether ISPs effectively meet the legal requirements, whether they provide the necessary information for consumers to make meaningful choices, and whether they observe the proportionality principle. At national level, the authorities competent for the above include the national telecommunication authorities on the one hand, and on the other, national data protection authorities. At EU level, relevant EU-level bodies include BEREC. The EDPS may also be able to play a role in this context.

82. In addition to monitoring the present level of compliance, given the relative novelty of the possibility of massive, real-time inspection of communications, some aspects related to the application of the framework that have been discussed in this Opinion require further more in-depth analysis and ulterior clarification. Guidance particularly relevant in several areas includes:

- Determining the inspection practices that are legitimate to ensure the smooth flow of traffic which may not require users' consent, such as, for example, the fight against spam. In addition to the intrusiveness of the monitoring applied, aspects such as, for example, the level of disturbance to the smooth flow of traffic that would otherwise occur, are relevant.

- Determining which inspection techniques can be carried out for security purposes, which may not require users' consent.

- Determining when monitoring requires individual's consent, notably the consent of all the users concerned, and the permissible technical parameters to ensure that the inspection technique does not entail processing of data that is not proportionate vis-à-vis its intended purposes.

- Furthermore in the three cases above, guidance may be needed regarding the application of the necessary data protection safeguards (purpose limitation, security, etc).

83. Given that the competences in this field are both national and EU, the EDPS considers that sharing views and experiences in order to find harmonised approaches to the above is essential. To achieve that, the EDPS suggest the creation of a platform or an expert group which should gather together representatives of national regulatory authorities, the Article 29 Working Party, the EDPS and BEREC. The first goal of this platform would be to develop guidance, at least on the items identified above, in order to ensure solid and harmonised approaches and the same playing field. The EDPS calls upon the Commission to organise this initiative.

84. Last but not least, both national authorities as well as their EU counterparts, including BEREC and the EU Commission must pay close attention to market developments in this field. From a data protection and privacy perspective, the scenario where ISPs engage on a routine basis in traffic management policies offering subscriptions based on filtering access to content and applications, would be highly problematic. If this were ever to happen, legislation would need to be put in place to address this situation.

VII. CONCLUSIONS

85. ISPs' increasing reliance on monitoring and inspection techniques impinges upon the neutrality of the Internet and the confidentiality of communications. This raises serious issues relating to the protection of users' privacy and personal data.

86. While the Commission's Communication on the open internet and net neutrality in Europe briefly touches on these issues, the EDPS feels that more should be done in order to come to a satisfactory policy on the way forward. In this Opinion he has therefore contributed to the ongoing policy debate on net neutrality, particularly on aspects related to data protection and privacy.

87. The EDPS considers that there is a need for national authorities and BEREC to monitor the market situation. This monitoring should result in a clear picture describing whether the market is evolving towards massive, real-time inspection of communications and issues related to complying with the legal framework.

88. Monitoring of the market should not go without further analysis of the effects of new practices in relation to data protection and privacy on the Internet. This Opinion outlines some areas that would benefit from clarification. While EU agencies and bodies such as BEREC, the Article 29 Working Party and the EDPS may be in a good position to clarify the conditions of application of the framework, the EDPS considers that the Commission has a duty to coordinate and steer the debate. Therefore, he calls upon the Commission to take an initiative involving all those stakeholders in a platform or a working group, with this goal. Among the issues needing further analysis, the following points should be addressed:

- Determining the inspection practices that are legitimate to ensure the smooth flow of traffic and which can be carried out for security purposes;

- Determining when monitoring requires individual's consent, notably the consent of all the users concerned, and the permissible technical parameters to ensure that the inspection technique does not entail processing of data that is not proportionate vis-à-vis its intended purpose.

- In the cases above, guidance may be needed regarding the application of the necessary data protection saf eguards (purpose limitation, security, etc.).

89. Depending on these findings, additional legislative measures may be necessary. In such a case, the Commission should put forward policy measures aiming at strengthening the legal framework and ensuring legal certainty. New measures should clarify the practical consequences of the net neutrality principle, as this has already been done in some Member States, and ensure that users can exercise a real choice, notably by forcing ISPs to offer non-monitored connections.

Done in Brussels, 7 October 2011

Peter HUSTINX
European Data Protection Supervisor