Opinion of the European Data Protection Supervisor

on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

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

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

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,

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, as last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009,

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, and in particular its Article 41,

HAS ADOPTED THE FOLLOWING OPINION

I. INTRODUCTION

1. The European Union is taking part in negotiations on the drafting of an Anti-Counterfeiting Trade Agreement (ACTA). These negotiations were launched in 2007 amongst an initial group of interested parties and then continued with a broader group of participants; to date those include Australia, Canada, the European Union, Japan, Korea, Mexico, Morocco, New Zealand, Singapore, Switzerland and the United States. The European Commission received a mandate from the Council to enter into these negotiations in 2008.

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

2. The EDPS acknowledges that the cross-border trade in counterfeit and pirate goods is a growing concern that often involves organized criminal networks, which calls for the adoption of appropriate cooperation mechanisms at international level in order to fight against this form of criminality.

3. The EDPS outlines that the negotiation by the European Union of a multilateral agreement that has as its core subject the enforcement of intellectual property rights raises significant issues as to the impact of the measures taken to combat counterfeiting and piracy on individuals' fundamental rights, and in particular their right to privacy and data protection.

4. In this respect, the EDPS particularly regrets that he was not consulted by the European Commission on the content of such an agreement. Acting on his own initiative, the EDPS has therefore adopted the current opinion based on Article 41(2) of Regulation (EC) No 45/2001[1] in view of providing guidance to the Commission on the privacy and data protection related aspects that should be considered in the ACTA negotiations.

II. STATE OF PLAY AND FORESEEN CONTENT OF ACTA

5. The 7th round of negotiations took place in Mexico on 26-29 January 2010, with a view to concluding an agreement in the course of 2010. However, to date no official draft of the agreement has been released.

6. The negotiations aim at adopting a new multilateral agreement designed to strengthen the enforcement of Intellectual Property Rights (IPR) and to combat counterfeiting and piracy. If adopted, this new agreement would create improved international standards as to how to act against large-scale infringements of IPR. The European Commission DG Trade has particularly outlined that "*the intended focus is on counterfeiting and piracy activities that significantly affect commercial interests, rather than on activities of ordinary citizens*".[2]

7. As to the content of the agreement, the *Summary of key elements under discussion* released by the European Commission DG Trade in November 2009 indicates that ACTA's goal of fighting piracy and counterfeiting will be pursued through three primary components: (i) international cooperation, (ii) enforcement practices, and (iii) definition of a legal framework for the enforcement of IPR in several identified areas, and in particular in the digital environment.[3] The foreseen measures will notably deal with legal procedures (such as injunctions, provisional measures), the role and responsibilities of Internet Service Providers (ISPs) in deterring copyright infringement over the internet, and cross-border cooperation measures to prevent goods from crossing borders. The information made public, however, only provides the general lines of the agreement and does not go into the details of any specific and concrete measures.

[1] 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, OJ 2001, L 8/1.
[2] See http://trade.ec.europa.eu/doclib/docs/2009/november/tradoc_145271.pdf, p. 2.
[3] See footnote 2 above.

8. The EDPS notes that even if the intended objective of ACTA is to pursue only large-scale infringements of IPR, it cannot be excluded that activities of ordinary citizens might be captured under ACTA, especially as enforcement measures take place in the digital environment. The EDPS stresses that this will require that appropriate guarantees are set forth to protect the fundamental rights of individuals. Moreover, data protection laws cover all individuals, including those who are potentially involved in counterfeiting and piracy activities; the combat of large-scale infringements will certainly also involve the processing of personal data.

9. In this respect, the EDPS strongly encourages the European Commission to establish a public and transparent dialogue on ACTA, possibly by means of a public consultation, which would also help ensuring that the measures to be adopted are compliant with EU privacy and data protection law requirements.

III. SCOPE OF EDPS COMMENTS

10. The EDPS strongly calls on the EU, and in particular the European Commission who received the mandate to conclude the agreement, to strike a right balance between demands for the protection of intellectual property rights and the privacy and data protection rights of individuals.

11. The EDPS emphasizes that privacy and data protection are core values of the European Union, recognised in Article 8 ECHR and Articles 7 and 8 of the EU Charter of Fundamental Rights[4], which must be respected in all the policies and rules adopted by the EU pursuant to Article 16 of the Treaty on the Functioning of the European Union (TFEU).

12. Furthermore, the EDPS stresses that any agreement reached by the European Union on ACTA must comply with the legal obligations imposed on the EU with respect to privacy and data protection law, as notably set forth in Directive 95/46/EC[5], in Directive 2002/58/EC[6] and in the jurisprudence of the European Court of Human Rights[7] and of the Court of Justice[8].

13. Privacy and data protection must be taken into account from the very beginning of the negotiations, not when the schemes and procedures have been defined and agreed and it is therefore too late to find alternative, privacy compliant solutions.

[4] Charter of Fundamental Rights of the European Union, OJ 2007, C 303/1.

[5] 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, OJ 1995, L 281/31 (further: Directive 95/46).

[6] 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 2002, C 201/37, as last amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ L 337/11 (further: Directive 2002/58).

[7] Interpreting the main elements and conditions set out in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) adopted in Rome on 4 November 1950, as they apply to different fields. See particularly the case law referred to elsewhere in this opinion.

[8] See in particular: Case C-275/06, *Productores de Música de España* (Promusicae), ECR [2008], p. I-271 and Case C-557/07, *LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten*, nyr.

14. In view of the little information made publicly available, the EDPS notes that he is not in a position to provide an analysis of the specific provisions of ACTA. In this opinion, the EDPS will therefore focus on depicting the potential threats to privacy and data protection of possible concrete measures that the agreement, as it has been reported, may raise in the two following areas: intellectual property rights enforcement in the digital environment (chapter IV), and international cooperation mechanisms (chapter V).

IV. INTELLECTUAL PROPERTY RIGHTS ENFORCEMENT IN THE DIGITAL ENVIRONMENT

IV. 1. The need to analyse the privacy/data protection implications of 'three strikes Internet disconnection policies'

15. According to the European Commission, ACTA will create a legal framework to fight piracy in the digital environment.[9] This framework will establish the conditions under which ISPs and other on-line intermediaries[10] may be held liable as a result of infringing copyright material running through their facilities. The framework may also provide for measures and remedies to be imposed upon Internet users as a result of uploading or downloading infringing copyright material. While the details of such framework have not been officially released, in view of the information available from different channels, it can be foreseen that it could include the imposition of obligations on ISPs to adopt 'three strikes Internet disconnection policies', also referred to as 'graduated response' schemes. Such schemes will allow copyright holders to monitor Internet users and identify alleged copyright infringers. After contacting the ISPs of the alleged infringer, ISPs would warn the user identified as infringer; he would be disconnected from Internet access, after first receiving three warnings.

16. At the same time as the ACTA negotiations, three strikes Internet disconnection policies are being implemented in some Member States such as France. They are also discussed in various EU forums such as the Stakeholders' Dialogue on illegal up - and downloading that currently takes place animated by DG MARKT, in connection with the adoption of the Commission's Communication enhancing the enforcement of intellectual property rights in the internal market.[11] Discussions on this topic also take place in the European Parliament in the context of the pending debate on a draft European Parliament Resolution on enhancing the enforcement of intellectual property rights in the internal market (referred to as 'Gallo report').

17. Such practices are highly invasive in the individuals' private sphere. They entail the generalised monitoring of Internet users' activities, including perfectly lawful ones. They affect millions of law-abiding Internet users, including many children and adolescents. They are carried out by private parties, not by law enforcement authorities. Moreover, nowadays, Internet plays a central role in almost all aspects of modern life,

[9] See footnote 2 above.

[10] The different on-line intermediaries can be defined according to their functional roles. However, in the real world intermediaries usually take on several of these functions. On-line intermediaries include: *(a) access providers:* users connect to the network by connecting to an access provider's server; (b) *network providers:* they provide the routers, *i.e.* the needed technical facilities for the transmission of data; (c) *host providers:* they rent space on their server, upon which users or content providers can upload content. Users may upload and download material to an online service, such as a bulletin or a P2P networks.

[11] Communication from the Commission to the Council, the European Parliament and the European Economic and Social Committee enhancing the enforcement of intellectual property rights in the internal market, Brussels, 11 September 2009, COM (2009) 467 final.

thus, the effects of disconnecting Internet access may be enormous, cutting individuals off from work, culture, eGoverment applications, etc.

18. Against this background, it is relevant to assess the extent to which these policies are in line with EU data protection and privacy legislation, and more in particular whether three strikes Internet disconnection policies constitute a necessary measure to enforce intellectual property rights. In that context, it should furthermore be analysed whether other, less invasive methods exist.

19. It is still unclear whether three strikes Internet disconnection policies will be part of ACTA. However, these policies are being considered also in other areas and they have - potentially - an enormous impact on the protection of personal data and privacy. For these reasons, the EDPS finds it necessary to discuss them in this opinion. Before performing the analysis just referred to, the EDPS will briefly describe the applicable legal data protection and privacy framework.

20. It should be noted that in addition to data protection and privacy, three strikes Internet disconnection policies raise concerns regarding other values such as due process and freedom of speech. However, this opinion will only address those issues that are related to the protection of personal data and privacy of individuals.

IV. 2. Three strikes Internet disconnection policies and the application of the EU data protection/privacy legal framework

How three strikes Internet disconnection policies may be set up

21. In a nutshell, under three strikes Internet disconnection policies copyright holders using automated technical means, possibly provided by third parties, would identify alleged copyright infringement by engaging in monitoring of Internet users' activities, for example, via the surveillance of forums, blogs or by posing as file sharers in peer-to-peer networks to identify file sharers who allegedly exchange copyright material.[12]

22. After identifying Internet users alleged to be engaged in copyright violation by collecting their Internet Protocol addresses (IP addresses), copyright holders would send the IP addresses of those users to the relevant Internet Service Provider(s) who would warn the subscriber to whom the IP address belongs about his potential engagement in copyright infringement. Being warned by the ISP a certain number of times would automatically result in the ISP's termination or suspension of the subscriber's Internet connection.[13]

The applicable EU data protection/ privacy legal framework

23. Three strikes Internet disconnection policies have to comply with the requirements stemming from the right to privacy, as laid down in Article 8 ECHR and Article 7 of the Charter of fundamental rights, and stemming from the right to data protection as laid down in Article 8 of the Charter of fundamental rights and Article 16 TFEU, and as elaborated in Directive 95/46 and Directive 2002/58.

[12] P2P technology is a distributed computing software architecture that enables individual computers to connect to and communicate directly with other computers.
[13] Examples of alternative sanctions would include limiting the Internet connection's functionality, for example, the speed of the connection, volume, etc.

24. In the EDPS view, the monitoring of Internet user's behaviour and further collection of their IP addresses amounts to an interference with their rights to respect for their private life and their correspondence; in other words, there is an interference with their right to private life. This view is in line with the case law of the European Court of Human Rights.[14]

25. Directive 95/46 is applicable[15] since the three strikes Internet disconnection policies involve the processing of IP addresses which - in any case under the relevant circumstances - should be considered as personal data. IP addresses are identifiers which look like a string of numbers separated by dots, such as 122.41.123.45. A subscription to an Internet access provider will give the subscriber access to the Internet. Every time the subscriber wishes to go onto the Internet, he will be attributed an IP address through the device he is using to access the Internet (a computer, for example).[16]

26. If a user engages in a given activity, for example, uploads material onto the Internet, the user may be identified by third parties through the IP address he/she used. For example, the user holding IP address 122.41.123.45 uploaded allegedly copyright infringing material onto a P2P service at 3 PM on 1 January 2010. The ISP will then be able to connect such IP address to the name of the subscriber to whom it assigned this address and thus ascertain his/her identity.

27. If one considers the definition of personal data provided in Article 2 of Directive 95/46, "*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"*[17], it is only possible to conclude that IP addresses and the information about the activities linked to such addresses constitutes personal data in all cases relevant here. Indeed, an IP address serves as an identification number which allows finding out the name of the subscriber to whom such IP address has been assigned. Furthermore, the information collected about the subscriber who holds such IP address ("he/she uploaded certain material onto the Web site ZS at 3 PM on 1 January 2010") *relates to*, *i.e.* is clearly about the activities of an identifiable individual (the holder of the IP address), and thus must also be considered personal data.

---

[14] See notably ECHR 26 June 2006, *Weber and Saravia v. Germany* (dec.), no. 54934/00, para 77 and ECHR 1 July 2008, *Liberty and others v the UK*, no. 58243/00.

[15] The Court of Justice takes a wide approach on the applicability of Directive 95/46, which provisions must be interpreted in the light of Article 8 ECHR. The Court of Justice stated in its judgement of 20 May 2003, *Rundfunk*, joint cases C-465/00, C-138/01 and C-139/01, ECR [2003], p. I-4989, para 68, that "*provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures*".

[16] 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.

[17] Recital 26 complements this definition: "*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; ...*".

28. These views are fully shared by the Article 29 Working Party which, in a document on data protection issues related to intellectual property rights stated that IP addresses collected to enforce intellectual property rights, *i.e.* to identify Internet users who are alleged to have infringed intellectual property rights, are personal data insofar as they are used for the enforcement of such rights against a given individual.[18]

29. Directive 2002/58 is applicable as well, as three strikes Internet disconnection policies entail the collection of traffic and communication data. Directive 2002/58 regulates the use of such data and provides for the principle of confidentiality of communications made over public communications networks and of the data inherent in those communications.

IV.3. Whether three strikes Internet disconnection policies constitute a necessary measure

30. Article 8 ECHR sets forth the principle of necessity pursuant to which any measure that infringes the right to privacy of individuals is only allowed if it constitutes a necessary measure within a democratic society to the legitimate aim it pursues.[19] The principle of necessity can also be found in Articles 7 and 13 of Directive 95/46 and Article 15 of Directive 2002/58.[20] The principle requires an analysis of the proportionality of the measure, which must be assessed on the basis of a balance of the interests involved, which is placed in the context of the democratic society as a whole.[21] It furthermore implies an assessment as to whether alternative measures exist which are less intrusive.

31. Although the EDPS acknowledges the importance of enforcing intellectual property rights, he takes the view that a three strikes Internet disconnection policy as currently known - involving certain elements of general application - constitutes a disproportionate measure and can therefore not be considered as a necessary measure. The EDPS is furthermore convinced that alternative, less intrusive solutions exist or that the envisaged policies can be performed in a less intrusive manner or with a more limited scope. Also on a more detailed legal level the three strikes approach poses problems. These conclusions will be explained below.

---

[18] Article 29 Working Party, Working Document on data protection issues related to intellectual property rights (WP 104), adopted on 18 January 2005. This Working Party was set up under Article 29 of Directive 95/46. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46 and Article 15 of Directive 2002/58. See also the Working Party's opinion 4/2007 on the concept of personal data (WP 136), adopted on 20 June 2007, notably on p. 16-17.

[19] Article 8 ECHR expressly refers to the requirement that any interference or restriction must be "*necessary in a democratic society*".

[20] Article 13 of Directive 95/64 only allows a restriction when it constitutes "*a necessary measure to safeguard: (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others*". Article 15 of Directive 2002/58 requires that "*such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC*".

[21] See also ECHR 2 August 1984, *Malone v. the United Kingdom*, Series A no. 82, p. 32, paras 81 and s. and ECHR 4 December 2008, *Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, paras 101 and s.

Three strikes approach policies are disproportionate

32. The EDPS wishes to emphasise the far-reaching nature of the imposed measures. The following elements must be mentioned in this regard:

(i) the fact that the (unnoticed) monitoring would affect millions of individuals and *all* users, irrespective of whether they are under suspicion.

(ii) the monitoring would entail the systematic recording of data, some of which may cause people to be brought to civil or even criminal courts; furthermore, some of the information collected would therefore qualify as sensitive data under Article 8 of Directive 95/46 which requires stronger safeguards.

(iii) the monitoring is likely to trigger many cases of false positives. Copyright infringement is not a straight 'yes' or 'no' question. Often Courts have to examine a very significant quantity of technical and legal detail over dozens of pages in order to determine whether there is an infringement.[22]

(iv) the potential *effects* of the monitoring, which could result in disconnection of Internet access. This would interfere with individuals' right to freedom of expression, freedom of information and access to culture, e-Government applications, marketplaces, email, and, in some cases, with work-related activities. In this context it is particularly important to realize that the effects will be felt not only on the alleged infringer, but all the family relatives that use the same Internet connection, including school children who use the Internet for their school activities.

(iv) 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). The EDPS already stated in a previous opinion his concerns regarding the monitoring of individuals by the private sector (*e.g.* ISPs or copyright holders), in areas that are in principle under the competence of law enforcement authorities.[23]

33. The EDPS is not convinced that the benefits of the measures outweigh the impact on the fundamental rights of individuals. The protection of copyright is an interest of right holders and of society. However, the limitations on the fundamental rights do not seem justified, if one balances the gravity of the interference, *i.e.* the scale of the privacy intrusion as highlighted by the above elements, with the expected benefits, deterring the infringement of intellectual property rights involving - for a great part - small scale intellectual property infringements. As indicated by the Opinion of Advocate General Kokott in *Promusicae*: "*It is ... not certain that private file sharing, in particular when it takes place without any intention to make a profit, threatens the protection of copyright sufficiently seriously to justify recourse to this exception. To what extent private file sharing causes genuine damage is in fact disputed*".[24]

[22] Courts may have to assess whether the material is indeed copyright protected, which rights have been infringed, if the use can be considered as a case of fair use, the applicable law, the damages, etc.

[23] EDPS Opinion of 23 June 2008 on the Proposal for a Decision establishing a multiannual Community programme on protecting children using the Internet and other communication technologies, OJ 2009, C 2/2.

[24] See the Case referred to in footnote 8, pt. 106.

34. In this context, it is also worth recalling the European Parliament's reaction to 'three strikes schemes' in the context of the review of the telecoms package, particularly Amendment 138 to the Framework Directive.[25] In this amendment it was laid down that any restriction to fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the ECHR and with general principles of Community law, including effective judicial protection and due process.[26]

35. In this view, the EDPS further underlines that any limitation to fundamental rights will be subject to careful scrutiny both at EU and national level. In this context, a parallel can be drawn with the Data Retention Directive 2006/24/EC[27], which derogates from the general data protection principle of deletion of data when they are no longer necessary for the purpose for which they were collected. This directive requires that traffic data are retained for the purpose of combating serious crime. It has to be noted that retention is only allowed for "serious crime", that the retention is limited to 'traffic data' which in principle excludes information about the content of communications, and that stringent guarantees are adduced. Nevertheless, doubts have been raised on its compatibility with fundamental rights standards; the Romanian Constitutional Court decided that blanket retention is incompatible with fundamental rights[28], and there is currently a case pending before the German Constitutional Court.[29]

The existence of other, less intrusive means

36. The findings above are strengthened by the fact that less intrusive means for achieving the same purpose exist. The EDPS insists that such less intrusive models should be investigated and tried.

37. In this context, the EDPS recalls that the amended Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services (referred to as 'Citizens Rights Directive'), which is part of the recently reformed telecoms package, contains certain rules and procedures to limit small scale copyright

[25] See Directive 2009/140/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009, L 337/37.

[26] The final wording of the so-called 138 amendment reads as follows: "Article 1.*3a. Measures taken by Member States regarding end-users access' to, or use of, services and applications through electronic communications networks shall respect the fundamental rights and freedoms of natural persons, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and general principles of Community law. Any of these measures regarding end-users' access to, or use of, services and applications through electronic communications networks liable to restrict those fundamental rights or freedoms may only be imposed if they are appropriate, proportionate and necessary within a democratic society, and their implementation shall be subject to adequate procedural safeguards in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms and with general principles of Community law, including effective judicial protection and due process. Accordingly, these measures may only be taken with due respect for the principle of the presumption of innocence and the right to privacy. A prior, fair and impartial procedure shall be guaranteed, including the right to be heard of the person or persons concerned, subject to the need for appropriate conditions and procedural arrangements in duly substantiated cases of urgency in conformity with the European Convention for the Protection of Human Rights and Fundamental Freedoms. The right to effective and timely judicial review shall be guaranteed.*"

[27] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, OJ 2006, L 105/54.

[28] http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html.

[29] http://www.bundesverfassungsgericht.de/pressemitteilungen/bvg09-124.html

infringement among consumers.[30] Such procedures include the obligation by Member States to produce standardised public interest information on various topics, specifically mentioning infringements of copyright and related rights, and their legal consequences[31]. Member States can then request ISPs to distribute it to all their customers, and to include it within their contracts.

38. The system is meant to inform and dissuade individuals from disseminating copyrighted information and engaging in infringing activities, while avoiding monitoring of internet usage and related privacy and data protection concerns. The Citizens Rights Directive must be implemented in May 2011; thus, such procedures are not in place yet. Therefore, there have been no opportunities to test their benefits yet. Thus, it seems premature to overlook the potential beneficial outcome of these new procedures and embrace instead 'three strikes disconnecting policies', which are far more limiting of fundamental rights.

39. In addition to the above, it should be recalled that Directive 2004/48/EC of 28 April 2004 on the enforcement of intellectual property rights provides for various tools to enforce intellectual property rights before courts (discussed below in paras 43 and s.).[32]

40. The IPRE Directive has only recently been transposed into Member States laws. So far there has not been sufficient time to evaluate whether its provisions are appropriate for the purposes of enforcing intellectual property rights. Therefore, any need to replace the current system based on court proceedings, which has not been tested yet, is at least doubtful. The above raises the inevitable question of why existing infringements cannot be appropriately addressed by existing civil and criminal penalties for copyright infringement. Thus, before proposing such policy measures, the Commission should produce reliable information showing that the current legal framework has failed to produce its intended effects.

41. Furthermore, it is unclear whether any serious thought has been given to alternative economic business models which would not involve the systematic monitoring of individuals. For example, if copyright holders demonstrate their losses due to P2P usage, right holders and ISPs might, for example, trial differentiated Internet access subscriptions where part of the price for a subscription with unlimited access is distributed to copyright holders.

---

[30] See Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, OJ 2009, L 337/11.

[31] In particular, Article 21(4) of Directive 2009/136/EC provides that "*Member States may require that the undertakings referred to in paragraph 3 distribute public interest information free of charge to existing and new subscribers, where appropriate, by the same means as those ordinarily used by them in their communications with subscribers. In such a case, that information shall be provided 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 rights, and their legal consequences (...).*" Furthermore, pursuant to Article 20(2),"*Member States may also require that the contract include any information which may be provided by the relevant public authorities for this purpose on the use of electronic communications networks and services to engage in unlawful activities or to disseminate harmful content, and on the means of protection against risks to personal security, privacy and personal data, referred to in Article 21(4) and relevant to the service provided*."

[32] OJ 2004, L 157/45 (further: IPRE Directive).

The possibility to perform targeted monitoring in a less intrusive manner

42. Apart from the use of completely different models, which as indicated should be investigated and tested, targeted monitoring could in any event be operated in a less intrusive manner.

43. The purpose of enforcing intellectual property rights can also be achieved by the monitoring of only a limited number of individuals suspected of engaging in non-trivial copyright infringement. The IPRE Directive provides some guidance in that respect. It sets forth the conditions under which authorities may order that personal data held by Internet access providers be disclosed for the purposes of enforcing intellectual property rights. Article 8 provides that ISPs may be ordered by competent judicial authorities to provide personal information that they hold about alleged infringers (e.g. information on the origin and distribution networks of the goods or services which infringe an intellectual property right) in response to a justified and proportionate request in cases of infringements on a *commercial scale*.[33]

44. Accordingly, the 'commercial scale' criterion is decisive. Pursuant to this criterion, monitoring may be proportionate in the context of limited, specific, *ad hoc* situations where well-grounded suspicions of copyright abuse on a commercial scale exist. This criterion could encompass situations of clear copyright abuse by private individuals with the aim of obtaining direct or indirect economic commercial benefits.

45. In practice, to make the above effective, copyright holders might engage in targeted monitoring of certain IP addresses in order to verify the scale of the copyright violation. This would mean that copyright holders would also be allowed to keep track of reports alleging infringement for the same purposes. Such information should only be used after having verified the significance of the infringement. For example, clear cases of major infringements as well as non-significant yet continuous infringements, over a certain period of time, for the purpose of commercial advantage or financial gain. The need for continuity within certain periods of time is emphasised and further explained below in the discussion related to the conservation principle.

46. This would mean that in such cases, the collection of information for the purposes of demonstrating alleged Internet abuse may be deemed proportionate and necessary for the purposes of preparing legal proceedings, including litigation.

47. The EDPS considers, as an additional guarantee, that the data processing operations aimed at gathering such type of evidence should be prior checked and authorised by national data protection authorities. These views are based on the fact that the data processing operations would present specific risks to the rights and freedoms of individuals in the light of their purposes, *i.e.* carrying out enforcement actions which could eventually be criminal and in the light of the sensitive nature of the data collected. The fact that the processing involves monitoring of electronic communications is an additional factor that calls for enhanced supervision.

48. The EDPS considers that the 'commercial scale' embodied in the IPRE Directive is a very appropriate element to set the limits of the monitoring in order to respect the

[33] This is further confirmed in Recital 14 of the IPRE Directive.

principle of proportionality. Furthermore, there does not appear to be reliable evidence showing under the criteria set forth under IPRE that effective legal action against copyright infringement proves not possible or ineffective. For example, reports such as from Germany, where since 2008, following the transposition of the IPRE Directive, there have been about 3,000 court orders pursuant to which ISPs have disclosed to courts the subscriber information of 300,000 subscribers, seem to suggest the opposite.

49. In sum, since the IPRE Directive has only been in force for two years, it is difficult to understand why legislators would move from the criteria embodied in this Directive to more intrusive methods when the EU is just beginning to test those recently adopted. For the same reason it is also difficult to understand the need for replacing the current court based system by other type of measures (in addition to raising questions of due process, which are not addressed here).

IV.4. Compliance of three strikes Internet disconnection policies with more detailed data protection provisions

50. There are other more specific legal reasons why the three strikes approach is problematic from a data protection point of view. The EDPS would like to highlight the doubtful legal ground for the processing, which is required by Directive 95/46, and the obligation contained in Directive 2002/58 to discard log files.

Legal ground for processing

51. Three strikes approach schemes entail the processing of personal data, some of which will be used for the legal or administrative procedures towards cutting Internet access to repeated infringers. From this perspective, such data qualifies as sensitive data under Article 8 of Directive 95/46. Article 8(5) establishes that "*Processing of data relating to offences, criminal convictions or security measures may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law...*"

52. In this context, it is pertinent to recall the Article 29 Working Party document mentioned before, which discusses the issue of processing judicial data.[34] The Working Party states 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*".[35] While the collection of targeted, specific evidence, particularly in cases of serious infringements may be necessary to establish and exercise a legal claim, the EDPS fully shares the views of the Article 29 Working Party on the lack of legitimacy of wide scale investigations involving the processing of massive amounts of data of Internet users.

[34] See paragraph 28 of this Opinion.
[35] Emphasis added.

53. The discussion on the principle of proportionality described above and the 'commercial scale' criterion are relevant to determine in which conditions the collection of IP addresses and related information will be legitimised.

54. ISPs might try to legitimise the processing carried out by copyright holders by inserting clauses in their customer's contracts allowing the monitoring of their data and the cutting of their subscriptions. By entering into such contracts, customers would be deemed to have agreed to the monitoring. However, this practice raises first the basic question as to whether individuals can give consent to ISPs for a data processing that will be carried out not by the ISP but by third parties which are not under the 'authority' of the ISP.

55. Second, there is the question of the validity of consent. Article 2(h) of Directive 95/46 defines consent as "*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*". An important point is that in order to be valid, consent, whatever the circumstances in which it is given, must be a freely given, specific and informed indication of the data subject's wishes, as defined in Article 2(h) of the Directive. The EDPS has serious doubts as to whether individuals asked to consent to the monitoring of their Internet activities will have the opportunity to make a genuine choice - especially because the alternative will be having no Internet access, thus potentially jeopardising many other areas of their life.

56. Thirdly, it is highly questionable whether any such monitoring could ever be considered *necessary* for the performance of a contract to which the data subject is a party, as required in Article 7 (b) of Directive 95/46, since the monitoring is obviously not an object of the contract entered into by the data subject, but only a means for the ISP to serve other interests.

Discarding of log files

57. Under Directive 2002/58, more in particular its Article 6, traffic data such as IP addresses may only be collected and stored for reasons directly related to the communication itself, including billing, traffic management and fraud prevention purposes. Afterwards, the data must be erased. This is without prejudice to the obligations under the Data Retention Directive which, as discussed, requires the conservation of traffic data and its release to police and prosecutors to aid in the investigation of a **serious crime only**.[36]

58. In accordance with the above, Internet service providers should discard any log file revealing Internet users' activities that is no longer required for the above purposes. Taking into account that log files are not necessary for billing purposes, it would appear that three or four weeks should be sufficient for ISP for traffic management purposes.[37]

59. This means that, when contacted by copyright holders, unless such contact occurred within the limited period outlined above, ISPs should not have the log files linking

[36] See paragraph 35 of this Opinion.

[37] Traffic management includes the analysis of computer network traffic in order to optimize or guarantee performance, lower latency and/or increase usable bandwidth.

the IP addresses to the relevant subscribers. Retaining the log files beyond such period should only be done for justified reasons within the scope of the purposes provided by law.

60. In practical terms this means that, unless carried out very quickly, copyright holder's requests addressed to IPSs will not be able to be fulfilled, simply because the ISP will no longer have the information. This in itself sets the boundaries of what is meant by acceptable monitoring practices described in the above section.

Risks of spill over effects

61. The EDPS is furthermore concerned not only about the privacy and data protection impact of three strikes Internet disconnection policies but also about their spill over effects. If three strike Internet disconnection policies are allowed, they could be a slippery slope towards legitimizing even more massive surveillance of Internet users' activities, in different areas and for different purposes.

62. The EDPS urges the Commission to ensure that ACTA does not go further and against the current EU regime for enforcement of IPRs, which respects fundamental rights and freedoms and civil liberties, such as the protection of personal data.

V. DATA PROTECTION CONCERNS IN RESPECT OF INTERNATIONAL COOPERATION MECHANISMS

63. One of the means put forward by ACTA participants in order to tackle the issue of IPR enforcement is to enhance international cooperation, with a number of measures that would allow for the effective enforcement of intellectual property rights in the jurisdictions of ACTA signatories.

64. In view of the information available, it can be foreseen that a number of the measures planned for ensuring enforcement of intellectual property rights will involve international sharing of information about alleged IPR infringements amongst public authorities (such as custom authorities, police and justice) but also between public and private actors (such as ISPs and IP right-holders organisations). Such data transfers raise a number of issues from a data protection viewpoint.

V.1. Are the data exchanges envisaged in the context of ACTA legitimate, necessary and proportionate?

65. In the current state of the negotiations' process in which a number of concrete data processing elements remain either undefined or unknown, it is impossible to verify whether the proposed framework of measures is in accordance with fundamental data protection principles and EU data protection law.

66. It can be questioned first whether data transfers to third countries in the context of ACTA are legitimate. The relevance of adopting measures at international level in that field can be questioned as long as there is no agreement within the EU member

states over the harmonisation of enforcement measures in the digital environment and the types of criminal sanctions to be applied.[38]

67. In view of the above, it appears that the principles of necessity and proportionality of the data transfers under ACTA would be more easily met if the agreement was expressly limited to fighting the most serious IPR infringement offences, instead of allowing for bulk data transfers relating to any suspicions of IPR infringements. This will require defining precisely the scope of what constitutes the 'most serious IPR infringement offences' for which data transfers may occur.

68. Moreover, particular attention should be paid to the persons involved in the data exchanges, and whether data will only be shared amongst public authorities or if they will also involve exchanges between private actors and public authorities. As outlined earlier in this opinion, the involvement of private actors in an area that is in principle under the competence of law enforcement authorities raises a number of concerns.[39] The conditions under which private actors will be involved in collecting and exchanging with public authorities personal data relating to IPR infringements should be strictly limited to specific circumstances, with appropriate guarantees.

V.2. Applicable data protection law governing data transfers in the context of ACTA

General regime for data transfers

69. The general data protection framework applicable in the EU is set forth in Directive 95/46. Articles 25 and 26 of Directive 95/46 define the regime applicable for transfers of data to third countries. Article 25 requires that transfers are only done to countries that ensure an adequate level of protection, or otherwise such transfers are in principle prohibited.

70. The level of adequacy afforded by third countries is assessed on a case-by-case basis by the European Commission, who issued several decisions recognising adequacy to a number of countries following a thorough analysis from the Article 29 Working Party.[40]

71. The EDPS notes that most of the participants to ACTA are not part of the list of countries providing adequate data protection drawn up by the Commission: with the exception of Switzerland and - in specific circumstances - Canada and the US, all other participants to ACTA are not recognised as providing an adequate level of protection. This means that for data to be transferred from the EU to these countries one of the conditions of Article 26(1) of Directive 95/46 must be fulfilled or appropriate safeguards must be adduced by the parties at the data transfer in accordance with Article 26(2) of the Directive.

---

[38] A proposal on criminal sanctions is currently under discussion in the Council, COM (2006) 168 of 26 April 2006.

[39] See paragraphs 32 and 52 of this Opinion. See also the EDPS Opinion of 11 November 2008 on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, OJ 2009, C 128/1.

[40] See Adequacy decisions granted by the European Commission to Argentina, Canada, Switzerland, US Safe Harbor and US authorities in PNR context, Guernsey, Isle of Man, and Jersey; available at http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm.

Specific regime for data transfers in the field of criminal law enforcement

72. While Directive 95/46 constitutes the main data protection instrument in the EU, its scope is currently limited as it expressly excludes activities concerning, *inter alia*, the activities of the State in the area of criminal law (Article 3). Data exchanges for the purpose of criminal law enforcement will therefore fall outside the scope of Directive 95/46 and will be subject to the general data protection principles set forth in the Council of Europe Convention No 108 and its additional Protocol to which all EU member states are a party.[41] In addition, the rules adopted by the EU concerning police and justice cooperation in the field of criminal matters that are set forth in the Council Framework Decision 2008/877/JHA will apply.[42]

73. These instruments also pose as a principle that there must be an adequate level of data protection in the third country to which data are to be transferred. A number of derogations are provided, in particular when the third country provides adequate safeguards. Similarly to data exchanges under Directive 95/46, data exchanges in the field of criminal law enforcement will therefore require that appropriate safeguards are adduced between the parties to the data transfer for such transfer to take place.

Towards a new regime for data transfers

74. In the near future, new common rules for data protection applicable to all fields of activities of the EU can be expected to be adopted by the EU on the basis of Article 16 TFEU. This means that in a few years there might be a comprehensive EU data protection framework that sets out coherent rules for data protection across all fields of activities of the EU, which will impose the same level of safeguards and guarantees to all data processing activities. As was outlined by Viviane Reding[43], Commissioner for Justice, Fundamental Rights and Citizenship, this new framework should work as a single "modern and comprehensive legal instrument" for data protection in the EU. Such a framework is particularly welcomed as it would bring more clarity and consistency as to the rules applicable in the EU in respect of data protection.

75. In an international context, the EDPS also points at the Resolution on International standards for the protection of personal data and privacy adopted recently by data protection authorities, which is a first step towards establishing global data protection standards.[44] The International Standards include a number of data protection safeguards similar to those stated in Directive 95/46 and Convention No 108. Although the international standards have no binding force yet, they do provide useful guidance as to the data protection principles that can be voluntarily applied by third countries so that their legal framework is compatible with EU standards. The EDPS believes that ACTA signatories should also take into account the principles laid down in the International Standards when processing personal data from the EU.

---

[41] Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, adopted in Strasbourg on 28 January 1981, and Council of Europe, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

[42] Council Framework Decision 2008/877/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ 2008, L 350/60.

[43] See Answers to European Parliament questionnaire for Commissioner-designate Viviane Reding, p.5, http://www.europarl.europa.eu/hearings/static/commissioners/answers/reding_replies_en.pdf.

[44] Resolution adopted in Madrid in November 2009.

V.3. Necessity of implementing appropriate safeguards for protecting data transfers from the EU to third countries

What form the safeguards shall take in order to effectively protect data transfers to third countries?

76. If the necessity of transferring personal data to third countries is demonstrated, the EDPS stresses that the European Union should negotiate with third country recipients - in addition to the agreement on ACTA itself - specific instruments that contain appropriate data protection guarantees to govern the exchange of personal data.

77. Appropriate data protection safeguards should usually be set forth in a binding agreement between the EU and the third country recipient, by which the receiving party undertakes to respect EU data protection law and to provide individuals with the same rights and remedies as granted under EU law. The need for a binding agreement stems from Article 26(2) of Directive 95/46 and Article 13(3)(b) of the Framework decision and is furthermore supported by the existing practice of the EU of concluding specific agreements to allow specific data transfers to third countries.[45]

78. Similarly, under the draft International Standards the recipient may be required to guarantee that he will afford the required level of protection for the transfer to take place. These guarantees could also take the form of a contractual commitment.

Content of the safeguards to be adduced by ACTA signatories in respect of personal data transfers

79. The EDPS particularly stresses that international exchanges of information for law enforcement purpose are particularly sensitive from a data protection viewpoint, as such a framework could legitimise massive data transfers in a field where the impact on individuals is particularly serious, and where strict and reliable safeguards are all the more needed.

80. The EDPS outlines that specific conditions and safeguards can only be defined on a case-by-case basis in the light of all the parameters of the data exchanges. For the purpose of guidance, the EDPS is however highlighting below some of the principles and safeguards that must be adduced by third party recipients for the transfers of data to take place:

- It must be verified what is the legal justification under which the data processing activities take place (i.e. are the processing operations based on a legal obligation, on consent from the data subjects, or on any other valid justification?), and whether data transfers respect the initial purpose of data collection. No transfers should occur outside the scope of the specified purpose.

- The amount and types of personal data to be exchanged should be clearly specified and minimised to what is strictly necessary to achieve the purpose of the transfer.

[45] For example agreements of Europol and Eurojust with the US, PNR agreement, Swift agreement, agreement between the EU and Australia on the processing and transfer of European Union-sourced passenger name record (PNR) data by air carriers to the Australian customs service.

The personal data collected and transferred may notably include the IP address of Internet users, the date and time of the suspected offence, and the type of offence. The EDPS recommends that data are not linked to any specific individual during the investigation phase, and recalls that identification of a suspected person should only occur in accordance with the law and under the control of a judge. In this view, the EDPS outlines that data relating to IPR infringements and suspicions of infringements are a special category of data the processing of which is usually restricted to law enforcement authorities and requires applying additional safeguards. The persons authorised to process data relating to IPR infringements and suspicions of infringements and the conditions for processing these data must therefore be specifically defined in accordance with existing data protection law.

- The persons among whom the data may be shared must be clearly set out and onward transfers to other recipients should in principle be prohibited, unless onward transfers are necessary for a specific investigation. This limitation is particularly crucial as the designated recipients should not be unduly sharing information with non-authorised recipients.

- The EDPS presumes that ACTA will not only foresee cooperation between public authorities, but that it will also give enforcement tasks to private organisations (such as ISPs, copyright holders' organisations, etc.). In the latter case, the conditions and level of involvement of private organisations in the enforcement of IPR must be carefully assessed, in the sense that ACTA measures should not give a *de facto* right to ISPs and IP right-holder organisations to monitor users' behaviour online. Furthermore, the processing of personal data by private organisations in the context of law enforcement should only take place upon an appropriate legal basis. It is also important to clarify whether private organisations will be obliged to cooperate with the police and the extent of such cooperation. This should in any case be limited only to "serious crimes", the definition of which will also need to be laid down precisely since not all infringements of IPR shall be considered as being serious crimes.

- The method used for exchanging personal data must be clearly chosen, in particular it should be specified whether it will be done through a push system - e.g. ISPs and IP right-holders organisations would transfer under their control a number of data to third parties, such as police and law enforcement authorities, located abroad - or a pull system - e.g. police and law enforcement authorities would have direct access to databases of private parties or to databases where information is centralised. As was already outlined in the context of PNR, a push system is the only option compliant with data protection principles from an EU data protection perspective as it entitles the EU sender, who is most likely the data controller, to exercise control over the transfer of data[46].

- The time during which personal data will be retained by recipients must be specified, as well as the purpose for which such retention is necessary. Such retention period should be proportionate in view of the purpose to be achieved, meaning that data should be removed or deleted when they are no longer needed to achieve that purpose.

[46] See Article 29 Working Party Opinion 4/2003 on the Level of Protection ensured in the US for the Transfer of Passengers' Data, WP78, 13 June 2003.

- The obligations imposed on data controllers in third countries should be clearly set forth. Oversight mechanisms and/or enforceable accountability mechanisms must be guaranteed so that there are effective recourses and sanctions against data controllers in case of undue processing or other relevant incidents. Furthermore, redress mechanisms should be put in place so that individuals may lodge a complaint before an independent data protection authority and so that they may seek an effective remedy before an independent and impartial tribunal.[47]

- The instrument entered into between the parties should clearly specify the rights of data subjects with respect to their personal data when such data are processed by a third party recipient so as to guarantee that they have effective means of enforcing their rights in respect of a processing carried out abroad.

- Transparency is furthermore crucial, and parties to the data protection instrument must agree on how they will inform data subjects on the data processing that is taking place as well as on their rights and how to exercise them.

VI. CONCLUSIONS

81. The EDPS strongly encourages the European Commission to establish a public and transparent dialogue on ACTA, possibly by means of a public consultation, which would also help ensuring that the measures to be adopted are compliant with EU privacy and data protection law requirements.

82. In the course of the ongoing negotiations on ACTA, the EDPS calls on the European Commission to strike a right balance between demands for the protection of intellectual property rights and the right to privacy and data protection. The EDPS emphasizes that it is particularly crucial that privacy and data protection are taken into account from the very beginning of the negotiations before any measure is agreed upon so as not later on having to find alternative privacy compliant solutions.

83. While intellectual property is important to society and must be protected, it should not be placed above individuals' fundamental rights to privacy, data protection, and other rights such as presumption of innocence, effective judicial protection and freedom of expression.

84. Insofar as the current draft of ACTA includes or at least indirectly pushes for three strikes Internet disconnection policies, ACTA would profoundly restrict the fundamental rights and freedoms of European citizens, most notably the protection of personal data and privacy.

85. The EDPS takes the view that three strikes Internet disconnection policies are not necessary to achieve the purpose of enforcing intellectual property rights. The EDPS is convinced that alternative, less intrusive solutions exist or, at least, that the envisaged policies can be performed in a less intrusive manner or at a more limited scope, notably through the form of targeted *ad hoc* monitoring.

[47] See Opinion of the European Data Protection Supervisor on the Final Report by the EU-US High Level Contact Group on information sharing and privacy and personal data protection, 11.11.2008.

86. The three strikes Internet disconnection policies are also problematic on a more detailed legal level in particular as the processing of judicial data, notably by private organisations, must be based on an appropriate legal basis. The operation of three strikes schemes may further entail the storage of log files on a longer term, which would be contrary to existing legislation.

87. Furthermore, as far as ACTA involves exchanges of personal data between authorities and/or private organisations located in the signatory countries, the EDPS calls on the European Union to implement appropriate safeguards. These safeguards should apply to all data transfers made in the context of ACTA - whether they are in the field of civil, criminal, or digital law enforcement - and should be in accordance with the data protection principles set forth in Convention No 108 and Directive 95/46. The EDPS recommends that such safeguards take the form of binding agreements between EU senders and third country recipients.

80. The EDPS further wishes to be consulted on the measures to be implemented in respect of the data transfers that will take place under ACTA in order to verify their proportionality, and that they guarantee an adequate level of data protection.

Done in Brussels, 22 February 2010

(signed)

Peter HUSTINX
European Data Protection Supervisor