Opinion of the European Data Protection Supervisor

on the proposal for a Council Decision on the Conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America

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,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

I.1. The EU legislative process on ACTA

1. On 24 June 2011, the Commission put forward a proposal for a Council Decision on the conclusion of the Anti-Counterfeiting Trade Agreement ('ACTA' or the 'Agreement') between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America[3].

[1] OJ L 281, 23.11.1995, p. 31.
[2] OJ L 8, 12.01.2001, p. 1.
[3] Commission proposal for a Council Decision on the conclusion of the Anti-Counterfeiting Trade Agreement between the European Union and its Member States, Australia, Canada, Japan, the Republic of Korea, the United Mexican States, the Kingdom of Morocco, New Zealand, the Republic of Singapore, the Swiss Confederation and the United States of America, COM(2011)380 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

2. The Agreement aims at tackling the enforcement of intellectual property rights ('IP rights') by developing a common approach to enforcement and facilitating cooperation at international level. Chapter II contains measures in several areas of the law, namely in the field of civil enforcement (section 2), border measures (section 3), criminal enforcement (section 4), and enforcement of intellectual property rights in the digital environment (section 5). Chapter III contains measures to improve enforcement practices, and Chapter IV deals with international cooperation.

3. ACTA was adopted unanimously by the Council in December 2011[4] and signed by the European Commission and 22 Member States[5] on 26 January 2012. According to Article 40 of the Agreement, ACTA will enter into force after ratification by six signatory states. However, to enter into force as EU law the Agreement must be ratified by the EU, which means approval by the European Parliament under the consent procedure for international commercial agreements[6] and ratification by Member States under their constitutional procedures. The European Parliament's vote on ACTA is scheduled to take place in the course of 2012 in plenary session.

I.2. State of play of ACTA in the EU

4. Growing concerns have been expressed over the last months about ACTA[7]. This has led the European Commission to announce on 22 February 2012 its intention to refer the agreement to the Court of Justice of the European Union for an opinion[8]. Such procedure is foreseen in Article 218(11) of the Treaty on the Functioning of the European Union ('TFEU')[9].

5. On 4 April 2012, the Commission decided that it would ask the Court the following question: '*Is the Anti-Counterfeiting Trade Agreement (ACTA) compatible with the European Treaties, in particular with the Charter of Fundamental Rights of the European Union?*'.[10] In case the outcome would be negative, Article 218(11) TFEU makes it clear that *'the agreement envisaged may not enter into force unless it is amended or the Treaties are revised'*.

6. However, the referral of the Agreement to the Court of Justice by the Commission would not automatically suspend the consent procedure currently under way in the European Parliament. After discussion in the International Trade Committee of the

[4] The text of the agreement, in its latest version of the Council of 23 August 2011, is available at: http://register.consilium.europa.eu/pdf/en/11/st12/st12196.en11.pdf.
[5] Germany, Cyprus, Estonia, the Netherlands and Slovakia have not signed it yet.
[6] Pursuant to Article 218(6) TFEU.
[7] See amongst others: http://euobserver.com/9/115043; http://euobserver.com/871/115128; https://www.bfdi.bund.de/bfdi_forum/showthread.php?3062-ACTA-und-der-Datenschutz, http://www.bbc.co.uk/news/technology-17012832.
[8] Statement by Commissioner Karel De Gucht on ACTA (Anti-Counterfeiting Trade Agreement), http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/128.
[9] Article 218(11) TFEU provides that 'A Member State, the European Parliament, the Council or the Commission may obtain the opinion of the Court of Justice as to whether an agreement envisaged is compatible with the Treaties. Where the opinion of the Court is adverse, the agreement envisaged may not enter into force unless it is amended or the Treaties are revised.' According to Article 107(2) of the Rules of procedures of the Court of Justice, '[t]he Opinion may deal not only with the question whether the envisaged agreement is compatible which the provisions of the Treaties but also with the question whether the Union or any Union institution has the power to enter into that agreement.'.
[10] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/354&format=HTML&aged=0&language=EN&guiLanguage=en.

European Parliament, it was decided to proceed with the vote on the Agreement in accordance with the planned schedule[11].

I.3. The reasons for a second EDPS Opinion on ACTA

7. In February 2010, the EDPS issued an Opinion on his own initiative in order to draw the attention of the Commission on the privacy and data protection aspects that should be considered in the ACTA negotiations[12]. While negotiations were being conducted confidentially, there were indications that ACTA would contain online enforcement measures having an impact on data protection rights, notably the three strikes mechanism[13].

8. The EDPS at the time focused his analysis on the lawfulness and proportionality of this type of measure and concluded that the introduction in ACTA of a measure that would involve the massive surveillance of Internet users would be contrary to EU fundamental rights and in particular the rights to privacy and data protection, which are protected under Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the EU[14]. The EDPS furthermore underlined the safeguards needed for international exchanges of personal data in the context of IP rights' enforcement.

9. Now that the text of the proposed agreement on ACTA has been made public[15], the EDPS considers it appropriate to issue a second Opinion on ACTA to assess some of the provisions contained in the Agreement from a data protection perspective, and by doing so to provide specific expertise that could be taken into consideration in the ratification process. Acting on his own initiative, the EDPS has therefore adopted the current Opinion based on Article 41(2) of Regulation (EC) No 45/2001 in view of providing guidance on the privacy and data protection issues raised by ACTA.

II. SCOPE OF EDPS COMMENTS

10. The EDPS acknowledges the legitimate concern of ensuring the enforcement of IP rights in an international context. However, while more international cooperation is needed for the enforcement of IP rights, the means envisaged for strengthening their enforcement must not come at the expense of fundamental rights of individuals, and in particular their rights to privacy and data protection. The EDPS has therefore called upon the European Commission, at the time the Agreement was under negotiation, to strike a right balance between, on the one hand, demands for the protection of IP rights, and, on the other hand, the privacy and data protection rights of individuals[16]. The need for an appropriate balancing of rights in the context of IP enforcement was recently once

[11] See http://www.neurope.eu/article/parliament-halts-sending-acta-court-justice.
[12] Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement (ACTA), OJ C 147, 5.06.2010, p.1.
[13] 'Three strikes Internet disconnection policies' or 'graduated response' schemes allow copyright holders, or entrusted third parties, to monitor Internet users and identify alleged copyright infringers. After contacting the Internet Service Providers ('ISPs') of the alleged infringer, ISPs would warn the user identified as infringer, and he would be disconnected from Internet access after having received three warnings.
[14] Charter of Fundamental Rights of the European Union, OJ C 303, 14.12.2007, p. 1.
[15] See footnote 3.
[16] See paragraph 10 of the EDPS Opinion of 22 February 2010 on ACTA.

again re-affirmed by the Court of Justice of the European Union on 19 April 2012 in the case *Bonnier Audio AB*[17].

11. As will be developed further below, the EDPS notes that the provisions relating to enforcement of IP rights on the Internet raise concerns from a data protection perspective. As said, the Court of Justice is asked to clarify whether the provisions of ACTA are in line with the European Treaties, in particular the Charter of Fundamental Rights. The analysis in the present Opinion takes a more focused perspective as it assesses the compatibility of the Agreement only in respect of EU law on privacy and data protection, and it also checks whether the provisions of the Agreement may open the door to possible undue and unacceptable side effects on individuals' privacy and data protection if they are not implemented correctly. In other words, does the Agreement give the right incentives for the legislators of the EU and in the Member States to take the needs for protection of the right to data protection into account? The present Opinion should in any event not be understood as pre-empting the advice of the Court of Justice.

12. Although this Opinion is focused on the enforcement measures set forth in the digital chapter of ACTA, it also assesses other provisions of the Agreement where relevant. It builds upon the analysis made in the previous EDPS Opinion on ACTA, which remains fully valid in respect of the threats to privacy and data protection caused by the widespread monitoring of Internet users and the safeguards needed for international exchanges of personal data in the context of IP rights' enforcement. It will therefore not repeat in full the previous analysis but make reference to it where applicable. After assessing the threats to data protection and privacy raised by the envisaged enforcement mechanisms in the digital environment (section III), a more specific analysis of some of the provisions of the Agreement will be conducted from a data protection perspective (section IV).

III. THREATS TO DATA PROTECTION AND PRIVACY RAISED BY THE ENVISAGED ENFORCEMENT MECHANISMS IN THE DIGITAL ENVIRONMENT

III.1. Measures foreseen in the digital chapter of ACTA (Chapter II, section 5)

13. Chapter II, section 5 of ACTA contains a number of measures aimed at facilitating the enforcement of IP rights in the digital environment. Although these measures are designed to help fight against all forms of IP rights infringements, including trademarks, the protection of copyright is at the core of that chapter.

14. The digital chapter of ACTA contains two measures specifically designed for facilitating enforcement of IP rights in an online environment, which contracting parties have the possibility but not the explicit obligation to introduce into their legal system: (i) a mechanism by which an online service provider may be ordered by *'a competent authority'* to disclose the identity of a suspected subscriber directly and expeditiously to a right holder[18], and (ii) the promotion of *'cooperative efforts within the business community to effectively address trademark and copyright or related rights infringement'*[19].

[17] See Case C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB*, judgment of 19 April 2012.
[18] Article 27(4) of ACTA.
[19] Article 27(3) of ACTA.

15. The first type of measure aims at ensuring the disclosure to right holders of the identity of individuals whose behaviour is suspected to infringe IP rights online. Under such mechanism, online service providers would be placed under an obligation to disclose personal data of some of their subscribers to right holders if given criteria are fulfilled, subject to the intervention and control of an authority.

16. The second type of measure is not as self-explanatory as the first one and it is unclear what types of measures the reference to *'promote cooperative efforts within the business community*' entails. A recital in the preamble of ACTA is more specific in indicating that such cooperation is desirable '*between service providers and right holders to address relevant infringements in the digital environment*'. Many contracting parties in whose territory certain types of voluntary enforcement cooperation mechanisms have already been implemented between ISPs and right holders are likely to contend that these mechanisms would fall under the scope of Article 27(3) of the Agreement. These include various forms of voluntary enforcement cooperation mechanisms, such as three strikes mechanisms, blocking and filtering of peer to peer traffic, or the blocking of websites allegedly infringing copyrights.

III.2. Why are such mechanisms problematic from an EU data protection perspective?

17. The Internet facilitates the exchanges, in various manners[20], of content covered by copyright; some of these exchanges concern lawful exchanges of protected works while others relate to unlawful creation and exchanges of content covered by copyright. Amongst all IP rights, copyright is certainly the right whose enforcement on the Internet raises the most challenges and privacy concerns, in particular in view of the large number of individuals who may be affected by copyright enforcement measures directed to activities carried out online.

18. Many of the measures that could be implemented in the context of Articles 27(3) and 27(4) of ACTA would involve a form of monitoring of individuals' use of the Internet, whether by detecting actual IP rights infringements or by trying to prevent any future infringements. In many cases, the monitoring would be carried out by right holders or right holders' associations and third parties acting on their behalf, although they often seek to delegate such task to ISPs[21].

19. Measures that entail the generalised monitoring of Internet users activities are highly invasive of the individuals' private sphere. They are usually carried out unnoticed and may affect millions of individuals or even all users, irrespective of whether they are under suspicion. They may involve the monitoring of electronic communications exchanged over the Internet and the review of the content of individuals' Internet communications, including emails sent and received, websites visited, files downloaded or uploaded, etc. Furthermore, such monitoring usually entails the systematic recording of data, including the IP address of suspected users. All this information can be linked to a particular individual through the ISP, who can identify the subscriber to whom the suspected IP address was allocated. It therefore constitutes personal data as defined in Article 2 of the Data Protection Directive 95/46/EC[22].

[20] For example, through peer-to-peer networks, web download, streaming, etc.
[21] This is particularly the case in the context of preventing infringements, where right holders have for example required ISPs to implement filtering tools which involve the monitoring by ISPs of all users' behaviour on the Internet.
[22] See also paragraph 27 of the EDPS Opinion of 22 February 2010 on ACTA.

20. As a result, these measures will often constitute an interference with individuals' fundamental rights and freedoms, such as the rights to privacy, to data protection, and to the confidentiality of communications, protected in Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the Charter of Fundamental Rights of the EU[23].

21. The lawfulness of specific enforcement measures that interfere with fundamental rights and freedoms must be assessed in the light of the criteria set forth in Article 8(2) the European Convention on Human Rights[24] and Article 52 of the Charter of Fundamental Rights of the EU[25]. They require that any limitation is provided for by law and necessary and proportionate to the legitimate aim it pursues. Furthermore, measures that involve the processing of personal data must be in compliance with data protection law, which, inter alia, requires that they are grounded on a valid legal basis.

22. As concerns the necessity of a specific enforcement measure interfering with one or several fundamental rights, it must first be demonstrated how this measure responds to a pressing need in society. It must furthermore be considered whether other less intrusive alternatives are available or could be envisaged[26].

23. The assessment of the proportionality of a specific enforcement measure must be done on a case-by-case basis and in the light of fundamental rights with which it may interfere. In order to perform such an assessment, it is necessary that the measure is sufficiently precise and well defined in order to assess its concrete impact on the sharing of data as well as on other fundamental rights[27]. Furthermore, in the context of IP rights enforcement, the measure must be proportionate in response to an individualised infringement of IP rights; a measure that aims at preventing IP rights infringements in general would not be proportionate.

24. Two aspects are particularly important for assessing the proportionality of a measure aimed at enforcing IP rights: (i) the scale and depth of any monitoring of Internet use and of Internet users, and (ii) the scale of the IP rights infringements against which such a measure is directed.

25. A targeted form of monitoring by right holders would be legitimate if the processing is carried out in the context of specific, current or forthcoming judicial proceedings, to establish, make or defend legal claims. However, the generalised monitoring followed by the storage of data on a general scale for the purpose of enforcing claims, such as the scanning of the Internet as such, or all the activity in P2P networks, would go beyond what is legitimate. Such general monitoring is especially intrusive to individuals' rights and freedoms when it is not well defined and there is no limitation to it, in scope, in

[23] See EDPS Opinion of 7 October 2011 on net neutrality, traffic management and the protection of privacy and personal data, OJ C 34, 08.02.2012, p. 1.

[24] Article 8(2) provides that *'There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.'.

[25] Article 52(1) provides that *'Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.'*.

[26] See para. 42 and seq. of the EDPS Opinion of 22 February 2010 on ACTA.

[27] See Opinion of the Advocate General M. Pedro Cruz Villalón, Case C-70/10, *Scarlet Extended SA v SABAM*, 14 April 2011, para.66 and 68.

time, and in terms of persons concerned[28]. As a consequence, the indiscriminate or widespread monitoring of Internet user' behaviour in relation to trivial, small-scale not for profit infringement would be disproportionate and in violation of Article 8 ECHR, Articles 7 and 8 of the Charter of Fundamental Rights, and the Data protection Directive[29].

III.3. The current EU legal framework

26. From an EU perspective, the provisions of ACTA must be read in the light of the EU current legal order on the protection of fundamental rights and its legal framework regarding enforcement of IP rights, data protection, as well as the liability regime of Internet intermediaries. The enforcement measures contained in the digital chapter of ACTA should therefore be subject to the limitations of the EU legal order.

27. In the EU, the fundamental rights to privacy and data protection have been further elaborated in primary EU law, in Article 16 TFEU, and secondary EU legislation, in Directive 95/46/EC and the e-Privacy Directive 2002/58/EC[30]. The rights to privacy and data protection must furthermore be interpreted in the light of the case law of the European Court of Human Rights[31] and of the Court of Justice.

28. The current EU legal framework on IP protection has been carefully crafted with a view to respect other fundamental rights such as the rights to privacy and data protection. The IPRE Directive[32], and to a certain extent Directive 2001/29/EC[33], currently set forth the conditions for the enforcement of IP rights in civil procedures. Furthermore, the enforcement measures provided in ACTA should also respect the special liability regime of ISPs as set forth in the e-commerce Directive 2000/31/EC[34] and the obligations and limitations set forth on ISPs in the Data Retention Directive 2006/24/EC[35].

29. There is, however, no harmonisation at EU level concerning criminal sanctions and procedures for the enforcement of IP right, since no consensus could be reached at EU level. It remains therefore a field of national competence where such balancing of rights must be done at national level[36].

---

[28] See in particular Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgement of 24 November 2011, and Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, judgment of 16 February 2012.

[29] See para 31 to 34 of the EDPS Opinion of 22 February 2010 on ACTA.

[30] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37.

[31] Interpreting the main elements and conditions set out in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms adopted in Rome on 4 November 1950.

[32] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, L 195, 2004-06-02, p. 16.

[33] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 22.6.2001, p. 10–19.

[34] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'), OJ L 178, 17.7.2000, p. 1.

[35] 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 L 105, 13.4.2006, p. 54.

[36] This is the reason why the criminal enforcement section of ACTA was negotiated directly by EU Member States and not by the Commission.

30. This need to strike a fair balance between the right to property and fundamental rights, such as the right to data protection, has been consistently underlined and refined by the European Court of Justice since the *Promusicae* ruling[37].

31. It is thus particularly crucial that the enforcement measures foreseen in ACTA are in line with the current EU legal framework related to IP rights enforcement, which respects this balancing of rights.

III.4. Impact of ACTA on future EU and Member States legal frameworks

32. Whilst Articles 27(3) and 27(4) of ACTA are phrased in such a way that the introduction of these types of measures would not be mandatory for contracting parties[38], it nonetheless clearly lays out the possibility for contracting parties, including the EU as well as its Member States, to do so. Although the use of permissive language, instead of a mandatory one, would appear less problematic, it does not alleviate the concerns raised by the introduction of such mechanisms, for a number of reasons.

33. The drafting of the Agreement which came out as a result of the negotiations lacks a sufficient level of precision and leaves much room for interpretation open to contracting parties. Such lack of precision is regrettable as the Agreement does not lay out with sufficient legal certainty the types of mechanisms that could be put in place as a result of entering into ACTA and the safeguards against the misuse of personal data or to protect the right of defence.

34. In principle, the measures to be adopted in the EU to strengthen digital enforcement further to entering into ACTA should remain within the frame of EU law and the respect of fundamental rights as they are guaranteed in the EU. However, there is a risk that ACTA will impact the future EU framework as new legislation and modifications to current EU law might be motivated by the ratification of ACTA along the lines of what has been agreed. Also the broad implementation of measures under these provisions in third countries under ACTA might have an influence on the legislative discussion within the EU. While the Commission is currently looking at revising the IPRE Directive, the ratification of ACTA may provide incentives to introduce voluntary cooperation enforcement mechanisms, although no consensus has been reached so far at EU level. It therefore seems premature for the EU to already commit on certain basic principles, especially in relation to cooperation mechanisms between stakeholders and ISPs, considering that there is disagreement on the principle of such schemes.

35. Furthermore, Member States may in the meantime go forward in introducing their own measures. The current deficiencies in the wording of the text together with the incentives provided to contracting parties over the implementation and design of enforcement mechanisms in the digital environment in their own territory are elements that will open the door for fragmented approaches within the EU, which in turn will run the high risk of inappropriate or insufficient respect of data protection requirements within the EU.

---

[37] See in particular Case C-275/06 *Promusicae* [2008] ECR I-271, paragraphs 62 to 68, Case C-70/10, *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, Judgement of 24 November 2011, paragraph 44, Case C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV*, judgment of 16 February 2012, paragraphs 42-44, and Case C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB*, judgement of 19 April 2012.

[38] Article 27(3) states that contracting parties 'shall endeavour to' and Article 27(4) uses the term 'may'.

36. In view of the above, the EDPS would have preferred an agreement that contains more precise terms and specific safeguards, which would have helped prevent any unwanted approaches.

IV. DETAILED ANALYSIS OF SPECIFIC PROVISIONS OF ACTA

IV.1. The scope of the digital chapter and the notion of 'commercial scale' should be clarified

37. In the digital chapter of the Agreement, it is envisaged that enforcement should take place primarily in accordance with the civil and criminal enforcement procedures set forth in the contracting parties' laws. Other enforcement mechanisms which are specific to the digital environment are provided in Articles 27(3) and 27(4), although it is unclear to which extent such other mechanisms would fit in the civil and criminal enforcement regimes of contracting parties or whether they would constitute *ad hoc* means of enforcement.

38. The digital chapter does not define with sufficient clarity the type of acts that would be subject to any enforcement procedures in the digital environment and whether these would include, or on the contrary exempt, activities of individuals carried out over the Internet for purely private purposes, such as private file sharing.

39. In this regard, it is particularly unclear whether only those activities carried out on a 'commercial scale' would be subject to the enforcement measures set forth in the digital chapter. The 'commercial scale' criterion is mentioned in the Agreement only in relation to criminal enforcement procedures (Article 23)[39] but not as concerns civil enforcement procedures or other enforcement procedures envisaged in the digital chapter. This appears to be contrary to the EU approach in Directive 2004/48/EC, which applies the notion of 'commercial scale' also in respect of civil and administrative enforcement measures[40]. Thus, it is insufficiently guaranteed in ACTA that only the activities that are on a 'commercial scale' would be subject to the enforcement measures envisaged in the digital chapter.

40. Additionally, Article 23 implies a criminalisation of certain acts carried out on the Internet, which shall be subject to penalties '*that include imprisonment as well as monetary fines sufficiently high to provide a deterrent to future acts of infringement*' (Article 24). It attempts to provide for the criminalisation of certain types of acts, such as 'wilful copyright piracy' or 'wilful related rights piracy' committed 'on a commercial scale', without however defining clearly which types of acts would constitute a criminal offence. Moreover, there is no linking of the application of criminal enforcement measures to those acts that are being recognised as criminal offences in the law of contracting parties. Article 23 therefore appears to create new categories of offences that would be subject to criminal enforcement, without however providing for any definition that would meet the standards of legal certainty required as concerns criminal sanctions.

41. This is all the more worrying since the notion of 'commercial scale' itself has not been defined with sufficient precision to provide legal certainty on the scope of enforcement measures in the digital environment in relation to acts carried out by individuals in the

[39] Article 23 provides that '*Each Party shall provide for criminal procedures and penalties to be applied at least in cases of wilful trademark counterfeiting or copyright or related rights piracy on a commercial scale'*.

[40] Recital 14 provides that 'The measures provided for in Articles 6(2), 8(1) and 9(2) need to be applied only in respect of acts carried out on a commercial scale. This is without prejudice to the possibility for Member States to apply those measures also in respect of other acts (...)'.

context of private use. Article 23 specifies in relation to criminal enforcement measures that *'acts carried out on a commercial scale include at least those carried out as commercial activities for direct or indirect economic or commercial advantage*'. However the notion of 'indirect' economic or commercial advantage is very broad and may be interpreted widely to cover a large range of activities carried out by individuals on the Internet for purely private purposes from which they do not generate any economic gain or benefit. Furthermore, Article 23 is not an exhaustive list of acts that would be deemed to fall under the notion of commercial scale (use of the term *'at least'*). This may contradict the interpretation given to the notion of 'commercial scale' in the EU, where it is considered that it *'would normally exclude acts carried out by end-consumers acting in good faith*'[41] and acts '*carried out by private users for personal and not-for profit purposes*'[42].

42. As a result, the EDPS underlines that the Agreement is unclear about the scope of enforcement measures in the digital environment, and whether they only target large-scale infringements of IP rights. He regrets that the notion of 'commercial scale' is not defined with sufficient precision and that acts carried out by private users for personal and not-for profit purpose are not expressly excluded from the scope of the Agreement.

IV.2. The injunction mechanism and the monitoring of Internet users by right holders

43. In order to strengthen the enforcement of IP rights in the digital environment, Article 27(4) of the Agreement foresees the possibility for contracting parties to set up a specific injunction mechanism directed at ISPs[43]. This injunction procedure would allow *'competent authorities'* to require ISPs to identify the person behind the IP address whose behaviour is being suspected of infringing IP rights and to disclose such information '*expeditiously*' to a right holder.

44. The use of such an injunction mechanism implies that the right holder would engage in some form of monitoring of the Internet usage to identify accounts that are *'allegedly used for infringement'*. This involves the processing of sensitive data relating to suspected offences or criminal convictions, which, pursuant to Article 8(5) of Directive 95/46/EC *'may be carried out only under the control of official authority, or if suitable specific safeguards are provided under national law'*. Whilst the processing by right holders of data relating to suspicions of IP rights infringement may be allowed for purpose of their own litigation under specific conditions, it should not extend beyond what is necessary and proportionate for such purpose.

---

[41] See recital 14 of Directive 2004/48/EC.

[42] European Parliament legislative resolution of 25 April 2007 on the amended proposal for a directive of the European Parliament and of the Council on criminal measures aimed at ensuring the enforcement of intellectual property rights (COM(2006)0168 - C6-0233/2005 - 2005/0127(COD)), OJ C 74E, 20.3.2008, p. 526. See also Opinion of the European Economic and Social Committee on the Proposal for a European Parliament and Council Directive on criminal measures aimed at ensuring the enforcement of intellectual property rights COM(2005) 276 final — 2005/0127 (COD), Official Journal C 256, 27/10/2007, p.0003-0007. In particular that *'private file sharing on the Internet or reproduction (or music remixes), or the representation of material or intellectual works amongst family members or private individuals for educational or experimental purposes are implicitly excluded from the proposed Directive's scope of application. It would be appropriate to spell out this exclusion'*.

[43] According to Article 27(4), a contracting party '*may provide, in accordance with its laws and regulations, its competent authorities with the authority to order an online service provider to disclose expeditiously to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement, where that right holder has filed a legally sufficient claim of trademark or copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights'*.

45. In this respect, as explained in section III.2 above, from a data protection viewpoint right holders would only be allowed to engage into targeted monitoring in the context of limited, specific, ad hoc situations where well-grounded suspicions of copyright abuse on a commercial scale exist.[44] Furthermore, in view of the specific risks to the rights and freedoms of individuals, such targeted monitoring should be subject to additional data protection safeguards, such as the prior checking or authorisation by the relevant national data protection authorities[45].

46. From a procedural perspective the processing of judicial data by private parties, in particular the disclosure by ISPs to right holders of personal data allowing the identification of a suspected subscriber for purpose of enforcement of IPR, should be done under the control of a judicial authority.[46] This is currently the case as concerns the disclosure of personal data in the context of civil litigation under the IPRE Directive, whose 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'. The involvement of judicial authorities is an essential part of the current EU system and crucial to ensure that enforcement takes place in respect of due process and fundamental rights.

47. However, it is unclear who would be the *'competent authorities'* entrusted with such an injunction power under Article 27(4) of the Agreement. The use of the vague notion of '*competent authorities*' does not provide much legal certainty that the disclosure of personal data under this provision would only take place under the control of judicial bodies. Quite to the contrary, this notion may also include administrative bodies which have been entrusted with specific quasi-judicial tasks without however being subject to all the guarantees of independence, impartiality and respect of the rights to the presumption of innocence and to a fair trial imposed upon judicial bodies.

48. Furthermore, the conditions to be fulfilled by right holders to be granted such an injunction are also not particularly satisfactory. The right holder must have *'filed a legally sufficient claim of trademark or copyright or related rights infringement*' and must seek such information *'for the purpose of protecting or enforcing those rights*'. This wording is significantly weaker than the one of the IPRE Directive, under which the injunction would only be granted under the conditions that the request is made *'in the context of proceedings concerning an infringement of an intellectual property right'*, and that it is *'justified and proportionate'*. Under the IPRE Directive, it is for the courts, on a case-by-case basis, to assess the facts and the gravity of the alleged wrongdoing, such as its scale and the privacy risks to individuals, in order to decide whether or not such information must be disclosed.

[44] See para 45 and seq. of the EDPS Opinion of 22 February 2010 on ACTA.

[45] Article 20 of Directive 95/46/EC enables Member States to determine data processing operations that are likely to present specific risks to the rights and freedoms of individuals and to require that these processing operations are subject to prior checking.

[46] Article 29 Working Party document, WP104, page 7: 'As stated in Article 8 of the Data protection Directive, processing of data related to offences, criminal convictions or security measures can be processed only under strict conditions as implemented by Member States. 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 or the request of communication of personal data detained by other actors such as ISPs (...). Such investigation falls within the competence of judicial authorities'.

49. The uncertainties in Article 27(4) may have a significant impact in the context of extra-territorial orders issued by foreign competent authorities to ISPs based in Europe. The current wording of the Agreement may legitimise orders from foreign non-judicial bodies to EU based ISPs to disclose information allowing identification of their EU-based Internet subscribers to right holders, even when these orders would be outside the scope of any ongoing legal proceeding. This means that the protection of the rights of individuals to which EU-based Internet subscribers would be entitled under EU law would no longer be properly ensured in such context.

IV.3. Enforcement cooperation mechanisms and the monitoring of Internet by ISPs

50. As explained in section III.1 above, Article 27(3) envisages the voluntary introduction of 'private' enforcement mechanisms that are based upon the voluntary cooperation between right holders and ISPs.

51. The extent and the form of their cooperation may vary: (i) in the context of three-strike schemes ISPs are usually required to identify their subscribers in order to pass on to them warnings which may lead to the termination of their agreement with them, (ii) ISPs are also asked by right holders to carry out on their behalf the monitoring of suspected behaviours on the Internet, such as for three-strike schemes or to monitor websites that would contain allegedly unlawful content, and (iii) they may furthermore be asked by right holders to implement technical tools to filter peer-to-peer traffic and to block allegedly unlawful content, which may amount to their monitoring of individuals and of their electronic communications on a large scale.

52. These forms of enforcement cooperation mechanisms which entail the processing by ISPs of personal data for the purpose of IP rights enforcement and/or the monitoring of individuals' behaviour, including electronic communications, on a large scale raise serious concerns from a privacy and data protection perspective. They furthermore may lead to the disconnection of Internet access or the blocking of websites, which may interfere with fundamental freedoms such as the freedom of expression, the freedom to receive or impart information and access to culture[47].

53. It must be ensured that the role that ISPs would be asked to undertake in the frame of enforcement cooperation mechanisms introduced either in new legislation or at the request of right holders in the form of private agreements is compatible with their rights and obligations under EU law as well as with the protection of personal data and privacy of individuals in the EU. The recent case law of the Court of Justice in respect of measures imposed on ISPs for the purpose of IP rights enforcement is particularly enlightening in clarifying the limits of what ISPs are allowed to do in the context of IP rights enforcement on the Internet under EU law.

54. First, in accordance with the current ISPs liability regime set forth in the E-commerce Directive, and in particular its Article 15(1)[48], no measure involving the carrying out of a general monitoring of the information going through their network can be imposed upon ISPs. In *Scarlet v Sabam*[49], the Court analysed the processing of data undertaken

[47] This is mentioned for reference but will not be discussed further as this Opinion only addresses the issues related to the protection of personal data and privacy of individuals.
[48] Article 15(1) of Directive 2000/31/EC provides that *'Member States shall not impose a general obligation on providers, when providing the services covered by Articles 12, 13 and 14, to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating unlawful activity'*.
[49] See footnote 37.

by an ISP that was asked to implement a filtering measure aimed at preventing infringements of IP rights. The Court observed that such a filtering measure would require an ISP to actively monitor all the data relating to its customers and to monitor all electronic communications conducted on its network, whether or not they are engaged in illegal downloading activities. The Court concluded that such filtering measure would result in a general monitoring obligation that is incompatible with Article 15(1) of the E-commerce Directive 2000/31/EC.

55. Second, these types of measures would go beyond the scope of the processing that ISPs can lawfully carry out under data protection law, and in particular under the e-Privacy Directive. There is no legal basis under the e-Privacy Directive and the Data Retention Directive 2006/24/EC that would allow ISPs to lawfully retain the links between individual IP addresses and Internet usage for the purpose of longer-term monitoring or analysis aimed at identifying "possible" IPR infringers[50]. Furthermore, the fact that ISPs may hold certain data does not mean that these data can be transferred to copyright holders for another purpose. In this respect, disclosure of information they retain under the Data Retention Directive is limited to competent national authorities *'for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law*'[51]. Moreover, the monitoring of electronic communications exchanged on their networks would violate the secrecy of communications as elaborated in Article 5 of the e-Privacy Directive, without however being justified by any of the exceptions provided in Article 15 of the e-Privacy Directive. Finally, the disclosure by ISPs of data relating to electronic communications to third parties without users' consent would be in breach of Article 5 of the e-Privacy Directive.

56. Third, as explained in section III.2 above, these types of measures may entail a monitoring of Internet users' activities that is disproportionate to the aim of enforcing IP rights. In this view, the Court held in *Scarlet v Sabam*[52] that a measure which involves the monitoring of all electronic communications that is not well defined and specific in terms of scope, time, and persons concerned would not respect the requirement that a fair balance be struck between IP rights and other fundamental rights and freedoms[53].

57. Finally, voluntary enforcement cooperation mechanisms should not be deployed as a means to circumvent the law. The EDPS considers that it is not sufficiently ensured that voluntary measures to be developed by private actors further to ACTA would not go beyond the right balance to be struck between IP rights and data protection.

IV.4. Cooperation and cross-border exchanges of data

58. Several provisions of ACTA provide for the international exchange of information, such as between border authorities (Article 29) and between public authorities (Article 34). ACTA's provisions on information sharing and cooperation are formulated in such a broad manner that it is particularly unclear what type of data could be exchanged and between whom. Such exchanges could cover any type of information, including personal data relating to suspicions of IP rights infringements. Furthermore, other

[50] See para.54 to 60 of the EDPS Opinion of 22 February 2010 on ACTA.
[51] See Article 4 of the Data Retention Directive, as well as Case C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v Perfect Communication Sweden AB*, judgement of 19 April 2012, para. 41.
[52] See footnote 37.
[53] See para. 45 and seq. of the judgement.

provisions of ACTA may entail the international transfer of information amongst private parties and/or between public and private parties (e.g. in the context of enforcement procedures envisaged in Article 11 and Article 27(4)).

59. First, the EDPS emphasises that all the procedures envisaged in the Agreement which would involve the processing of personal data of individuals within the scope of EU law must respect data protection laws; this protection covers all categories of individuals, regardless of their nationality or residence, including those suspected of or potentially involved in counterfeiting and piracy large-scale infringements.

60. As with any measure having an impact on the privacy and data protection rights of individuals, transfers of personal data in this context must meet the tests of necessity and proportionality. The EDPS has already stated in his previous Opinion that the principles of necessity and proportionality of the data transfers would be more easily met if the Agreement was expressly limited to fighting the most serious IP rights infringement offences, instead of allowing for bulk data transfers relating to any suspicion of such infringements[54]. This has not been followed up as the formulation of the Agreement is particularly unclear as to the scope of the enforcement procedures (as explained in section IV.1 above).

61. Furthermore, transfers of personal data to recipients located outside the EU must be done in accordance with data protection requirements. Articles 25 and 26 of Directive 95/46/EC set forth the conditions under which international transfers of personal data may be carried out. Specific rules apply in respect of data transfers in the field of criminal law enforcement, set forth in the Council of Europe Convention No 108 and its additional Protocol[55] and in the Council Framework Decision 2008/877/JHA[56]. All these rules are based on common principles, in particular that transfers to recipients located in countries that are not deemed to provide an adequate level of protection must be subject to the respect of additional safeguards laid out clearly in legally binding instruments (such as the amount and types of data transferred, restrictions on onward transfers, time limit for the retention of the data, oversight and effective redress mechanisms).

62. As a result, the EDPS underlines that the EU will need to enter into specific agreements with its trade partners to ensure adequate data protection safeguards for the exchange of personal data with recipients in these countries.

IV.5. The lack of appropriate safeguards in ACTA

63. Pursuant to Articles 27(2), 27(3) and 27(4) of the Agreement, the enforcement measures to be implemented in the digital environment must preserve 'fundamental principles, such as freedom of expression, fair process and privacy'. The EDPS underlines that a mere reference to these principles is not enough. Besides, it is unclear what 'fundamental principles' and 'fair process' refer to.

[54] See para. 67 of the EDPS Opinion of 22 February 2010 on ACTA.

[55] 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 the Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, Strasbourg, 8 November 2001.

[56] 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 L 350, 30.12.2008, p. 60.

64. At international level, freedom of expression and privacy are recognised as fundamental rights in the Universal Declaration of Human Rights, and not as mere 'principles'. Furthermore, the notion of 'fair process' does not correspond to any generally recognised human right. It appears to mix two different legal concepts, on the one hand the right to a fair trial (recognised in Article 10 of the Universal Declaration of Human Rights and Article 47 of the Charter of Fundamental Rights of the EU), and on the other hand, the notion of 'due process' (used for example in the US constitution as a means to protect any person against deprivation of life, liberty or property without due process of law).

65. It is noteworthy to underline that the European Union laid out precisely in the context of the review of the above-mentioned Directive 2002/21/EC the safeguards necessary for the implementation of measures touching upon end-users' access to, and use of, services and applications through electronic communications networks. They include in particular adequate procedural safeguards in conformity with the European Convention on Human Rights and general principles of Community law, including effective judicial protection, due process, the principle of the presumption of innocence and the right to privacy[57].

66. The EDPS underlines the benefits of an approach that lays out clearly the limitations and safeguards within which measures touching upon the use and monitoring of electronic communications networks may take place. It would therefore have been much better if ACTA had laid out clearly such safeguards.

V. CONCLUSION

67. While the EDPS acknowledges the legitimate concern of ensuring the enforcement of IP rights in an international context, a right balance must be struck between demands for the protection of IP rights and the rights to privacy and data protection.

68. The EDPS emphasizes that the means envisaged for strengthening enforcement of IP rights must not come at the expense of the fundamental rights and freedoms of individuals to privacy, data protection and freedom of expression, and other rights such as presumption of innocence and effective judicial protection.

69. Many of the measures envisaged in the Agreement in the context of enforcement of IP rights in the digital environment would involve the monitoring of users' behaviour and of their electronic communications on the Internet. These measures are highly intrusive

[57] Article 1(1)(b) of Directive 2009/140/EC, inserting a new paragraph (3a) into Article 1 of Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services (the so-called '138 Amendment'): '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.'.

to the private sphere of individuals and, if not implemented properly, may therefore interfere with their rights and freedoms to, *inter alia*, privacy, data protection and the confidentiality of their communications.

70. It should be ensured that any online enforcement measure implemented within the EU as a result of entering into ACTA is necessary and proportionate to the aim of enforcing IP rights. The EDPS underlines that measures that entail the indiscriminate or widespread monitoring of Internet user' behaviour, and/or electronic communications, in relation to trivial, small-scale not for profit infringement would be disproportionate and in breach of Article 8 ECHR, Articles 7 and 8 of the Charter of Fundamental Rights, and the Data Protection Directive.

71. The EDPS has furthermore specific concerns in relation to several provisions of the Agreement, in particular:

- the Agreement is unclear about the scope of enforcement measures in the digital environment envisaged in Article 27, and whether they only target large-scale infringements of IP rights. The notion of 'commercial scale' in Article 23 of the Agreement is not defined with sufficient precision, and acts carried out by private users for a personal and not-for profit purpose are not expressly excluded from the scope of the Agreement;

- the notion of 'competent authorities' entrusted with the injunction power under Article 27(4) of the Agreement is too vague and does not provide sufficient certainty that the disclosure of personal data of alleged infringers would only take place under the control of judicial authorities. Furthermore, the conditions to be fulfilled by right holders to be granted such an injunction are also not satisfactory. These uncertainties may have a particular impact in cases of requests from foreign 'competent authorities' to EU-based ISPs;

- many of the voluntary enforcement cooperation measures that could be implemented under Article 27(3) of the Agreement would entail a processing of personal by ISPs which goes beyond what is allowed under EU law;

- the Agreement does not contain sufficient limitations and safeguards in respect of the implementation of measures that entail the monitoring of electronic communications networks on a large-scale. In particular, it does not lay out safeguards such as the respect of the rights to privacy and data protection, effective judicial protection, due process, and the respect of the principle of the presumption of innocence.

Done in Brussels, 24 April 2012

(**signed**)

Giovanni BUTTARELLI
Assistant European Data Protection Supervisor