ACTA – report by the EDPS

I. Introduction

On 24 April 2012, the European Data Protection Supervisor (EDPS) issued an "Opinion 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 "Opinion").

This documents elaborates on the comments made by Mr. Anders Jessen, of DG Trade of the European Commission, at the LIBE meeting of 26 April 2012 to the Opinion. This is without prejudice to an official Commission position on the Opinion.

II. General Comments:

In this Opinion, the EDPS **a)** makes an assessment of some of the provisions contained in the Agreement from a data protection perspective, and **b)** provides an overview over the current legal framework for privacy and data protection, which could act as guidance on how such ACTA provisions are to be implemented in order to comply with the applicable data protection legislation in Europe.

Examples of the latter is the description of the functioning of the EU legal framework provided, inter alia in paragraphs 26 to 30 (EU rules on privacy and data protection), 45, 46 (EU rules on injunctions for the monitoring of internet users) or 53 to 56 (EU rules on cooperation mechanisms). In these sections, the EDPS provides its perspective of how the corresponding ACTA rules would be applied in Europe.

However, instead of presenting it as such, the Opinion concludes that that the EDPS has several concerns relating to ACTA which, in our view, are unfounded.

We note that the Opinion does not, as it has been publicly reported, say that ACTA is *per se* contrary to the rights to privacy and data protection established under EU law. Rather it concludes that due to a perceived lack of clarity in certain provisions and the alleged absence of specific safeguards, ACTA *could* be implemented in a manner that would be disproportionate and in breach of certain provisions of the Charter of Fundamental Rights and the Data Protection Directive.

Since, as it will demonstrated below, nothing in ACTA *requires* the EU to implement the agreement in a way as described in the general and specific concerns enumerated in paragraphs 68 to 71 of the Opinion, it would appear that the Opinion is in reality concerned, not with what ACTA does, but rather with the fact that ACTA doesn't explicitly constrain EU and national legislators from taking certain actions.

a) Erroneous assumptions

In order to arrive at it conclusion the EDPS makes two critical, and, in our view, erroneous assumptions.

- First, it fails to take into account most of the explicit and detailed safeguards ensuring a balance between intellectual property and other fundamental rights that are foreseen in ACTA such as privacy, data protection, fair process or proportionality (examples in the Preamble, in article 2.1, article 4, article 6, article 11, etc). Given the importance, and the straightforward wording, of these safeguards, such omissions are not understandable. In those cases where the EDPS does acknowledge some of these safeguards (article 27.2, 27.3 and 27.4, qualifying the provisions related to Internet), it summarily dismisses them without a clear justification (paragraph 64 of the Opinion). Few, if any international treaties, and certainly no other international agreement on intellectual property, contain so many and so precise safeguards of fundamental rights – not recognising this fact renders any analysis of ACTA incomplete. A list of such safeguards, most of them with direct or indirect relevance regarding the protection of privacy and data protection, is provided in Annex I;

- Second, it systematically assumes that the provisions of ACTA that leave room for some flexibility in their implementation, will be implemented in the EU in manners that are illegal and contrary to fundamental rights. This is a wrong and unjustified assumption which is rejected by general principles of law and by the letter of ACTA itself. ACTA explicitly requires that the optional or flexible provisions therein be implemented in compliance with fundamental rights and applicable domestic provisions (law and jurisprudence);

It is only by basing the Opinion on a selective analysis of ACTA and by assuming that ACTA would not be implemented in the EU through (existing) EU law, but instead through a systematically flawed implementation outside of the *acquis* that it is possible to reach the conclusions promoted by the EDPS, such as:

- that ACTA promotes strengthened enforcement at the expense of freedom of expression, privacy or data protection;
- that it allows or even promotes illegal practices such as systematic monitoring of internet use; or
- that it may allow the circumvention of EU data protection rules.

We dispute these conclusions. Furthermore, we will clarify below how the specific provisions identified in the Opinion (articles 23 and 27) only address matters that exist and are well defined in the existing EU and national law of Member States and do not promote or require any modification or implementation that would be contrary to such law.

b) Selective analysis of the agreement

We disagree with the selective analysis that has been made of the ACTA provisions with an impact on data protection and privacy matters. The Opinion overlooks provisions that address most of the expressed concerns and has flaws in terms of legal reasoning.

The most relevant omission for a report about data protection in ACTA regards the existence in the text of an article addressing "Privacy and Disclosure of Information". There is not a single reference in the Opinion to Article 4 ACTA and to the essential safeguards that it introduces and that are applicable to all the other provisions of the agreement, including those specifically targeted by the EDPS.

Article 4[1] ensures that the authorities of the ACTA members shall not disclose any information contrary to their own legislation, including, obviously all the rules applicable in the EU to the treatment of data protection and the right to privacy, regardless of whether they are foreseen in the Charter of Fundamental Rights, a European Directive or national legislation. These safeguards also protect against disclosure of information that would impede law enforcement, be contrary to the public interest or to legitimate commercial interests of entities concerned.

Another general, but important criticism to be made to the Opinion relates to the basic approach which underlies the analysis summarised by the statement *"ACTA measures to enforce IP rights in the digital environment could threaten privacy and data protection if not properly implemented"*[emphasis added].

In fact, the Opinion does not identify a specific illegality or incompatibility with EU legislation that may exist in any particular provision of ACTA but instead warns about the risk that there may be ways to implement certain ACTA provisions that may interfere with rights and freedoms such as privacy, data protection, due process or the presumption of innocence.

We find this approach problematic for a number of reasons. First, any legal measure, if wrongly implemented, can harm fundamental rights. Taking the argument to the extreme, the rule that obliges people to wear a car seat-belt can be criticised for being dangerous if badly implemented if it fails to provide sufficient safeguards preventing people from wearing it around their neck!

Second, it appears to require that, when negotiating international agreements, the Commission must not only ensure that the agreement can be implemented in a way compatible with EU law, but also that provisions are included into such agreements for the sole purpose of constraining EU and national legislators from taking certain action.

Third, it is a basic and general principle of law that if some rule has two interpretations, one that is fully respectful of fundamental principles (or even other laws) and another that is contrary, then the only valid interpretation is the one compatible with fundamental principles (or other laws).

---

[1]

ARTICLE 4
Privacy and Disclosure of Information

1. Nothing in this Agreement shall require a Party to disclose:

(a) information, the disclosure of which would be contrary to its law, including laws protecting privacy rights, or international agreements to which it is party;

(b) confidential information, the disclosure of which would impede law enforcement or otherwise be contrary to the public interest; or

(c) confidential information, the disclosure of which would prejudice the legitimate commercial interests of particular enterprises, public or private.

2. When a Party provides written information pursuant to the provisions of this Agreement, the Party receiving the information shall, subject to its law and practice, refrain from disclosing or using the information for a purpose other than that for which the information was provided, except with the prior consent of the Party providing the information.

Throughout the Opinion there is the view that ACTA rules do not *per se* infringe or contradict EU principles and laws but if, for some unclear, unjustified and unexplained reason the EU legislator would decide to implement such rules in a manner contrary to such EU laws and principles, then ACTA poses a threat to EU citizens.

This reasoning does, not only, disregard the above principle but also appears not to take into account that ACTA provisions are not directly applicable to EU citizens and companies and that such implementing rules need to be legally adopted by EU and/or national legislators, who are bound to the Treaties, including the Charter of Fundamental Rights, national Constitutions and other legislation in areas such as privacy, data protection, due process or the presumption of innocence.

III. Specific Comments

a) Erroneous reading of the provisions relating to "internet enforcement"

Equally important is the fact that ACTA itself provides such safeguards explicitly and in numerous provisions. Surprisingly, most of these safeguards, which introduce direct limitations to the way the ACTA provisions may be implemented in the European Union (as well as in other ACTA Parties) are not mentioned in the Opinion. Other safeguards, such as those included in article 27.2, 27.3 and 27.4, are partially referred to and summarily dismissed on the basis of being "unclear" – *cfr*. paragraphs 63 and 64 of the Opinion.

These safeguards, repeated in each of the provisions relating to "internet enforcement" are particularly relevant. Even if both the "cooperation clause" and the "information clause" of article 27.3 and 27.4 respectively, are only optional, ACTA mandates that, if these rules are to be implemented, they must comply, *inter alia*, with the laws and fundamental principles including those on data protection, privacy and fair process

We cannot stress enough the importance of such safeguards. These ensure – even if that would not be necessary in view of the general principle that forbids the illegal implementation of any legal provision - that the ACTA rules will never be implemented in a manner that violate European and Member States national legislation, inter alia, in the area of data protection, privacy or civil liberties.

The Opinion comes to the conclusion that there is such risk (paragraphs 13 to 25 of the Opinion) through a two step reasoning:

- first, by assuming that the only mechanisms available to implement article 27.3 and 27.4 will necessarily infringe data protection or privacy rules; and

- second, by ignoring or considering irrelevant the second part of articles 27.3 and 27.4.

Afterwards, the Opinion describes some of the current EU legal framework (paragraphs 26 to 30). This section is valuable to help understand how the ACTA provisions are already and will continue to be implemented in Europe. The problem is that, because the Opinion does not acknowledge that ACTA mandates its Parties to apply article 27.3 and 27.4 in a manner "*consistent with that Parties' law*" and fundamental principles, it then proceeds to warn about an alleged negative impact that an implementation which would disregard or even infringe such laws and principles.

However, there is nothing in ACTA promoting, suggesting or even allowing this kind of implementation, therefore we do not share such concerns.

b) Specific concerns in relation to several provisions of the Agreement

The Opinion analyses in some detail, the following provisions, in relation to which it highlights a number of concerns:

- *The lack of clarity 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.*

Once more, the explicit reference in article 27.3 and 27.4 to the need of being implemented in a manner "*consistent with the Parties' laws*" provides all the necessary legal certainty and clarity. Insofar as the implementation of these measures would require any of the three civil enforcement mechanisms that, in the EU can only be applied to infringements on a commercial scale (those foreseen in articles 6.1, 8.1 and 9.2 IPRED), then, that will remain unchanged and only infringements on a commercial scale will continue to allow for the possibility of obtaining the evidence foreseen in article 6.1 IPRED, of obtaining the information foreseen in article 8.1 IPRED or the provisional measures foreseen in article 9.2 IPRED.

The definition of "commercial scale" as established in article 23 ACTA has no impact whatsoever on the implementation of the Enforcement Directive in the EU. On the other hand, nothing in ACTA requires any provision of the Enforcement Directive to be modified or its implementation reviewed.

The Opinion also appears to indicate that ACTA introduces a novelty by criminalising certain acts carried out on the internet. This is not correct: piracy on a "commercial scale" has been a crime at least since the TRIPS Agreement of the WTO entered into force in 1996. It applies to all 154 Members of the WTO (although least-developed countries benefit from a waiver). Obviously, it applies to all EU Member States since 1996 or since they joined the WTO.

In line with this, ACTA contains criminal enforcement measures (the ones that contain a punitive element, such as a fine or a prison term) only for serious violations, made wilfully (i.e. which are committed with intention) and on a commercial scale.

The commercial scale concept with its definition referring to "*direct or indirect economic or commercial advantage*" has been firstly introduced in the EU law in the Rental and Lending Directive 92/100/EEC of 19 November 1992, codified in 2006 in Directive 2006/115/EC (recital 11). The same EU definition has been used in the above mentioned articles of the Enforcement Directive.

Then, this concept appears in TRIPS, Article 61 regarding criminal procedures, but without definition: "*Members shall provide for criminal procedures and penalties to be*

applied at least in cases of wilful trademark counterfeiting or copyright piracy on a commercial scale."[2]

In ACTA, the Member States (the criminal section was negotiated by them) proposed to define "commercial scale" based on the EU definition (Article 23.1 ACTA).

This concept has been interpreted and developed by jurisprudence and it should exclude *acts carried out by end consumers acting in good faith*. It has also been applied by national criminal courts of Member States in hundreds or even thousands of trials for crimes of piracy or counterfeiting.

The Opinion also questions whether ACTA is criminalising *activities carried out by individuals on the internet for purely private purposes from which they do not generate any economic gain or benefit*. Even if it is necessary to stress that the EU has not yet exercised competence in the area of IPR penal enforcement, our view is that such acts are not being criminalised by ACTA because they do not fall within ACTA's reference to acts on a commercial scale being *commercial activities for direct or indirect economic or commercial advantage*. An act by an individual for private purposes and no economic motivation or advantage should not be qualified as a commercial activity.

- *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;*

Once more, paragraphs 44 to 46 of the Opinion provide an explanation of the functioning of mechanisms to obtain from ISPs information to identify an alleged infringer. However, also here, the Opinion does not acknowledge that ACTA mandates its Parties to apply 27.4 in a manner "*consistent with that Parties' law*" and preserving "fundamental principles" and once more proceeds to warn about the "possibility" of such measures being implemented by non-judicial authorities in Europe.

The reference to the need for consistency with EU law contained in article 27.4, but also the principle contained in article 2.1 ACTA that *(e)ach Party shall be free to determine the appropriate method of implementing the provisions of this Agreement within its own legal system and practice* provide all the safeguards and legal certainty that the EU needs to continue granting such competence to judicial authorities.

On this matter, it may also be useful to clarify that, even if most ACTA Parties provide this competence to their judicial authorities, there was at least one country where it belongs to a body of the Administration which has certain quasi-judicial enforcement competences and thus, could not accept a narrower definition.

The same reasoning applies to the criticism made in the Opinion with regard to the conditions to be fulfilled by right-holders to benefit from the measure foreseen in article 27.4 ACTA. This provision is already implemented in Europe through the Enforcement Directive and the e-commerce Directive (article 15.2). We do not consider that the

[2] To be noted that the inclusion of the reference to "at least", which is criticised in the Opinion, is not introduced by ACTA but comes from the TRIPS Agreement (1994).

requirements foreseen in ACTA are weaker than those of the Enforcement or the e-commerce Directives and recall that principles of fairness, equity and proportionality[3] (article 6.2 and 6.3 ACTA) are also applicable.

In view of the above, but also having in consideration the above mentioned article 4 ACTA that strictly safeguards EU rules in case of information being exchanged between authorities of the ACTA parties, we do not share the Opinion's concern about any negative impact arising from requests by foreign non-judicial competent authorities in relation to EU-based ISPs. These will have to be made through an EU judicial authority and should only be authorised if in line with EU legislative requirements (including those described in paragraph 61 of the Opinion), as foreseen in ACTA.

- *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;*

This conclusion is incorrect and contradicted by the reading of article 27.3 ACTA, which makes express reference to the need for implementing cooperation in a manner "*consistent with [the] Party's law"*. As stressed above, it is not an option for ISP's to go beyond what is allowed in EU law without engaging in illegal practices and exposing themselves to the consequences of such act. ACTA does not promote, encourage or endorse such practices.

The Opinion lists in paragraph 51 a number of cooperation practices that may raise privacy and data protection concerns and appears to indicate that these are the only possible forms of cooperation between business stakeholders. This is incorrect on several grounds: First, some of those mentioned practices have only been introduced in certain Member States through national laws and not through corporate agreements. It is therefore not exact to mention them as examples of business cooperation. Second, there are certainly other examples of ways of implementing article 27.3: one of them is the model of Stakeholders Dialogues implemented by DG Internal Market since 2009, concerning both the *Sale of Counterfeit Goods over the Internet* and *Illegal Up- and Downloading (Online Copyright Infringement)*[4]. The Opinion makes no reference to this well established European model – and fully ACTA compatible - of promoting cooperative efforts between internet related businesses.

- *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.*

We have explained above our disagreement with this conclusion and consider that the Opinion either overlooks or summarily disregards the fact that such safeguards are included in ACTA – *cfr.* Annex I.

---

[3] Any decision made by an EU judicial authority will need to take into account the need for proportionality between the seriousness of the infringement, the interest of third parties and the applicable measures, remedies and penalties (article 6.3 of ACTA).

[4] http://ec.europa.eu/internal_market/iprenforcement/stakeholders_dialogues_en.htm

Additionally, the Commission has decided to refer ACTA to the European Court of Justice to ensure a detailed examination of whether ACTA is in line with European Fundamental Rights such as the freedom of expression and information or data protection and the right to property including that of intellectual property. The question put to the ECJ is: "*Is the Anti-Counterfeiting Trade Agreement (ACTA) compatible with the European Treaties, in particular with the Charter of Fundamental Rights of the European Union?*"

ANNEX I

Below are the main provisions and safeguards expressly introduced in ACTA to ensure that it is a balanced treaty, mandating the respect of fundamental rights and of the general legal framework that needs to be taken into account when implementing IPR enforcement provisions:

- *Preamble, recital 5:* ACTA will not create barriers to legitimate trade
- *Preamble, recital 6:* Need for balance between the rights and interests of right-holders, service providers and users, including in the digital environment
- *Preamble, recital 9:* Recognition of the principles of the Doha Declaration on Public Health
- *Article 1:* General obligation to comply with the TRIPS Agreement, including its entire system of safeguards. It also integrates in ACTA by reference all flexibilities which are not expressly derogated by specific provisions of ACTA
- *Article 2.1:* Freedom of Parties to implement the provisions of ACTA within their own legal system and practice
- *Article 2.3:* Specific incorporation of the principles and objectives of the TRIPS Agreement as stipulated in its articles 7 and 8 (includes promotion of innovation, dissemination of technology, the balance of rights and obligations, the protection of public health and nutrition and other important matters that need to be considered when protecting and enforcing IPR)
- *Article 3.2:* Safeguard against the need for Parties to enforce rights not protected under their law
- *Article 4:* Safeguard of privacy and data protection rules for public authorities
- *Article 6.1:* Safeguard against the abuse of ACTA provisions and the creation of barriers to trade
- *Article 6.2:* Fairness and equity of provisions, protection of the rights of all the parties
- *Article 6.3:* Principle of proportionality
- *Article 11:* Safeguard of confidentiality of information sources, (client-attorney) privilege, procession of personal data according to domestic law regarding information to be provided in civil litigation –
- *Article 12.4:* Providing of a security to safeguard defendants in application of provisional measures
- *Article 12.4:* Providing of compensation for undue provisional measures
- *Article 18:* Providing of a security to safeguard defendants against undue customs requests for action
- *Article 22:* Safeguard of laws on privacy and confidentiality regarding information to be provided to rightholders in customs procedures
- *Article 27.2:* Safeguard of laws and principles, including specifically on freedom of expression, fair process and privacy, as well as prevention of the creation of barriers to legitimate activities, including specifically electronic commerce regarding the implementation of enforcement measures in the digital environment
- *Article 27.3:* Safeguard of laws and principles, including specifically on freedom of expression, fair process and privacy, as well as the obligation to preserve legitimate competition regarding the optional provision to promote cooperation between digital environment businesses
- *Article 27.4:* Safeguard of laws (expressly mentioned twice in the same paragraph, once in the beginning and once in the end) and principles, including specifically

on freedom of expression, fair process and privacy, as well as prevention of the creation of barriers to legitimate activities, including specifically electronic commerce regarding the optional implementation of provisions to disclose information about online infringements

- *Article 27.8:* Safeguard of the Parties' exceptions, as well as rights, limitations or defences regarding enforcement measures against the circumvention of technological measures and electronic rights management information