Douwe Korff
Professor of International Law
London Metropolitan University
Calcutta House, Old Castle Street
London E1 7NT, United Kingdom
d.korff@londonmet.ac.uk

NOTE

on comments by the US Ambassador to the EU at the hearing of the EP's LIBE Committee on
"Data Protection in a Transatlantic Perspective"
(Brussels, 25 October 2010)

I. Introduction

1. The EU and the US are trying to reach an agreement on exchanges of personal data in the area of police and judicial cooperation in criminal matters, including in particular serious organised crime and terrorism. Crucial issues in this regard are:

   – Whether the US can provide adequate assurance to the EU (and through the EU to the MSs) that any personal data received from the EU[1] will be treated properly, in accordance with European data protection principles; and

   – What the effect of such an agreement would be on exisiting EU – US and Member States – US agreements in this field.

   The US Ambassador to the EU, Mr. W E Kennard, made a presentation on the above issues to the LIBE Ctee hearing in Brussels on 25 October 2010. This note contains summaries of some of his remarks, with comments from the author of this note, who gave a later presentation at the same hearing (see the handout by Douwe Korff). A summary is provided at the end, at IV (paras. 15 – 21).

2. Before addressing the above questions, I should note that the Ambassador stressed that Europe and the USA "shared their basic values"; this was also emphasised by Mme Le Bail.

   ***Comment**:* As also noted by Patrick Bleyer, in recent years, in its "War against Terrorism", the US has consistently betrayed these standards: in respect of the use of torture, "extraordinary rendition", illegal, secret detention sites, extra-judicial killings, serious violations of International Humanitarian Law (on the battlefield but also in Guantanamo Bay and worse in Baghram and elsewhere) - and in relation to interception of communications and other interferences with privacy. We may have seen this as a temporary abberation under the (second) Bush administration, but unfortunately these gross violations of basic international and democratic standards have not ended under the current Obama

[1] This Note generally concerns "personal data received [by the USA] from the EU". Note that this is not the same as "personal data on EU citizens" or even "EU citizens and -residents". If (as I believe it may be) the proposed EU – US Agreement is to cover the disclosure of all data by EU entities to US entities (and *visa versa*), then this will cover also, e.g., the disclosure by EU entities of data on illegal immigrants or even visa applicants (who may be anywhere in the world), and indeed data on (say) relatives or "contacts" of individuals in the EU (legally or otherwise) but who themselves are outside the EU. Data on such individuals is protected by EU law (and MSs national law) and it should be covered - and I assume will be covered - by the EU – US Agreement.

Presidency. It means that in assessing the more specific issues below, we simply cannot take bland assurances about "shared values" for granted.

NB After my presentation, Ms In 't Veld rightly pointed out that European Governments, too, had been complicit in the US crimes, which is of course true. But that is equally a betrayal of our basic standards. I hope that the Ambassador and Mme Le Bail did not mean to refer to the "shared values" of the human rights violators, but meant the shared values of democracy, the Rule of Law and human rights (and privacy).

II. <u>The adequacy of US-internal privacy law</u>

3. The first of the two issues noted in para. 1, above, hinges on two sets of further questions: (i) whether the US internal-legal privacy regime provides comparable protection to the European regime, as expressed in particular in COE Convention No. 108, in the main EC Data Protection Directive (Directive 95/46/EC) and in the [former] Third-Pillar arrangements such as the Europol- and Eurojust regimes; and if so, whether the US internal-legal regime can be said to be "equivalent" to the European regime, or at least "adequate" in terms of the Directive? And (ii) how strong, reliable and enforceable are the US undertakings under the proposed agreement?

   (i) whether the US internal-legal privacy regime provides comparable protection to the European regime?

4. The Ambassador repeatedly said that while there were "different approaches" in the EU and the US, both essentially provided proper protection of individuals. He said *inter alia*:

   > "We do not believe that there are serious shortcomings in either the US or the EU privacy regimes".

   And called for:

   > "A clear statement of mutual recognition [by the EU and the US] of each other's privacy regimes" as both being "adequate".

   To the extent that there were differences, he said that these regimes were not static, but rather needed to adjust to new circumstances and contexts:

   > "What we consider necessary and proportionate changes [over time]".

   In the end, Europe and the USA should agree to "meet in the centre".

   In the discussions, much was made of the US Privacy Act.

5. ***Comment***: It is quite simply untrue to suggest that in the area we were discussing US privacy law, and in particular federal law, comes even remotely close to the European standards. First of all, privacy law in the USA is a disparate patchwork of Federal and State-, common- and statute law. In some areas covered by federal law (such as cable tv), and in some State Constitutions and -laws, there are some protections that come somewhere near to the European standards. However, even in the better-protected areas (which mostly relate to private-sector controllers), standards do not really meet the European ones, especially when it comes to the (to us Europeans, absolutely core) requirement of "purpose-limitation". These laws also tend to contain sweeping exemptions in respect of disclosure of data by private-sector entities to law enforcement and anti-terrorist

agencies. Application of the laws and supervision over the private sector, in particular by the Federal Trade Commission, also fall short of European standards. The FTC, in particular, focusses excessively on data security and insufficiently on fair information and access rights. (On all of the above, see the Country Report referred to under the quote, below.)

Most importantly for any EU- US agreement, the (Federal) Privacy Act too does not really come close to the European standards, even when its terms are fully appicable (which in important respects they are not, as noted below):

> The Privacy Act governs how federal government agencies collect, use, and disseminate personal information of citizens. Like the FCRA [Fair Credit Reporting Act], the Privacy Act reflects a broad range of Privacy Guidelines. However, much of its impact has been limited through liberal employment of a "routine use" exception, which has allowed agencies to transfer personal information without violating the statute. A routine use is one that, "is compatible with the purpose for which it was collected." This exemption has been so liberally applied that agencies have crated "blanket routine uses" that apply to every information system housed at the agency. For instance, the Department of Defence has created a list of 16 such uses.[2] Thus, any system of records, no matter its content or context, can be disclosed for law enforcement, counterterrorism, historical archives, and for the "Information Sharing Environment." Specific systems of records may contain their own routine uses, meaning that discretionary information sharing can be quite broad and determined by the agency itself, rather than by Congress.
>
> (Chris Hoofnagle, *Country Report – United States of America*, produced for the EU Study led by Douwe Korf & Ian Brown, Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments. The Final Report on this study, an Executive Summary, and a series of country reports including the one on the USA, are all available from the European Commission website: http://ec.europa.eu/justice/policies/privacy/studies/index_en.htm.)

The PATRIOT Act further undermined such limited restrictions as there were (under the Privacy Act and basically all other laws) on the disclosure and use of data held by any public authority to law enforcement and anti-terrorist agencies. These agencies are actively "Hoovering up" massive amounts of personal data on non-US citizens (and sometimes, illegally, on US citizens too - which seems to be the only time there is an outcry over this in the USA), and they use them in truly scary programs, including "profiling" and "threat-" or "risk-assessment" programs, with little or no constraint or oversight. Yet the outcomes of this unfettered and unreliable processing of truly enormous amounts of personal data do affect (non-US) individuals, in that they feed into the US "no flight"- or "watch"-lists (or worse). (See Douwe Korff, Technologies for the Use of Images: Automated Processes of Identification, Behavioural Analysis and Risk Detection Control at the Airports, Spanish Data Protection Agency Seminar Presentation, June 2010. Available at SSRN: http://ssrn.com/abstract=1673772)

In addition, there is no "adequate" supervision over the collecting, storing, use and sharing of personal data by law enforcement and anti-terrorist agencies in the USA. Individuals involved in the limited supervisory arrangements relating to the Department of Homeland Security may be serious and willing to ensure a measure of privacy protection. However, they cannot impose stricter limitations than the law imposes. And crucially, they cannot be considered "independent" in the European sense - which the WP29 has stressed is a crucial aspect of "adequacy" (Note that a

[2] Department of Defense, Blanket Routine Uses, available at http://www.defenselink.mil/privacy/blanket_uses.shtml. [original footnote]

special additional protocol was adopted to the COE Convention 108 to remedy the absence of such a requirement from that instrument: this underlines the fundamental importance to Europeans of truly independent supervisory mechanisms). There is also a serious lack of transparency about what the DHS supervisory officials can really inspect, what they do really inspect, what they find, and what they manage to remedy or improve.

And of course, the Privacy Act is explicitly limited to data on US citizens and permanent residents. In that regard, the Ambassador referred to "the controversy over whether or not the Privacy Act protects EU citizens". That was disingenious: there is no "controversy" about this: the Privacy Act expressly and explicitly excludes its application to data on non-US citizens and -residents (unless one is talking about EU citizens living in the USA, which would be fatuous). The only "controversy" is about whether this exemption is justified; this in fact touches on a fundamental difference of approach between Europe and the USA in respect of human rights generally.

In Europe, it is seen as a basic principle of human rights law that such rights should be accorded to "everyone" within the power of the State in question,[3] and not just to nationals and residents: see the text of all the substantive articles of the ECHR and the EU Charter of Fundamental Rights. By contrast, the USA has used - I would say, abused - the fact that its constitutional rights are, as a matter of principle, not granted to non-US citizens and –residents, and denied extra-territorial effect, to allow detention without due process, torture and ill-treatment and denial of fair trials by US agencies, outside US territory, in flagrant breach of international human rights- and humanitarian law. The restriction of the Privacy Act (and the limitations on interception of communications) to US citzens and –residents is but one manifestation of this wider defect. That is what is "controversial".

Yet the USA does not intend to remove this limitation. The Ambassador went on to say:

> "Congress will not re-open the Privacy Act. It is not going to happen."

In my opinion, even if the Privacy Act were to be extended to data obtained from the EU (which it clearly will not be), this would not provide "adequate" (let alone "equivalent") protection to European data protection law, if such "adequacy" were to be assessed, as it should be, on the basis of the approach consistently followed in this regard by the Article 29 Working Party. (On that approach, see Douwe Korff, Data Protection Law in Practice in the EU, 2005, pp. 172 – 192, "*Determining whether there is "adequate" protection*".)

But without that, a data sharing agreement that is not itself fully enforceable in the US courts, and that cannot be invoked and relied on by any individual affected by it, in those courts, should be unthinkable. Let us now turn to that issue.

[3] The Convention actually uses the words "within their jurisdiction". However, the EuCtHR has given these words a substantive, not territorial meaning: it covers all places were the State Party exercises effective control over the individuals concerned. This is also confirmed by national courts applying the Convention. Thus, the British courts have accepted the applicability of the ECHR (through the UK Human Rights Act) to actions by British soldiers in Army detention centres in Iraq. This is why I use the words "within their power" in the text above. This European approach is in direct contrast to the US "Guantanamo" approach to US Constitutional rights, which excludes individuals outside the country (and who are not US citizens) from the protection of the Constitution.

(ii) how strong, reliable and enforceable are the US undertakings under the proposed agreement?

6. The aim of the negotiations is, apparently, to reach a "binding international agreement" on EU – US data exchanges in the area covered by the Agreement. But we should be clear by what is meant by that.

7. First of all, it is useful to clarify some terminology. In particular, in international legal terms, any "binding agreement" between States or other bodies with international legal personality (such as the EU) that is intended to have international legal effect constitutes a "treaty", and should be applied in accordance with the Vienna Convention on the Law of Treaties (VCLT). The Agreement that is being prepared undoubtedly will be a treaty in this generally-accepted international-legal sense.

However, in the US, the term "treaty" is given a narrower meaning, and some other terms ("Congressional-Executive Agreement" and "Sole Executive Agreement") are also used. The last of these need not concern us here. In respect of the other two ("treaties" in the narrow US-legal sense and "Congressional-Executive Agreements"), it may suffice to note that the former require the "advice and consent" (but in practice only the consent) of two-thirds of the Senate, whereas the latter can be based on the concurrence of a simple majority of both houses of Congress; this takes the form of a Federal statute which must pass both houses of Congress. The President can choose which option to follow. However, in either case, an agreement only comes into effect after the President ratifies the instrument (after the appropriate consent or concurrence). (See: F L Kirgis, International Agreements and U.S. Law, ASIL Insight, 1997, available from: http://www.asil.org/insigh10.cfm)

In practice, the great majority of international agreements that the USA enters into these days take the form of a Congressional Executive Agreement:

> Historically, congressional-executive agreements have been made for a wide variety of topics, ranging from postal conventions to bilateral trade to military assistance. The North American Free Trade Agreement and the General Agreement on Tariffs and Trade are notable examples of congressional-executive agreements.
>
> (M J Garcia, International Law and Agreements: Their Effect Upon U.S. Law, Congressional Research service, 2010, available from: http://www.fas.org/sgp/crs/misc/RL32528.pdf)

If the EU and the US were to reach agreement on the text of the proposed Agreement, the US President is likely to seek to have it endorsed as a Congressional Executive Agreement, and would ratify it after both houses passed the relevant statute (but it would be useful for the LIBE Committee to have this clarified explicitly). Upon exchange of the instruments of ratification, it would then indeed become binding on both parties - and would constitute a treaty in terms of international law. It would be binding on the EU and on the USA in international law, and any violation of any of the terms of the agreement by either party would constitute an internationally wrongful act, for which the other party could demand reparation or redress.

Moreover, domestically, in the USA, the Agreement would have the status of a federal law. However, that in itself says little: we still have to look at the effect of the Agreement in domestic US law, and at the question of who could invoke its provisions in the US courts.

8. This effect of (provisions in) an international agreement in US law depends on whether the agreement as a whole, or specific provisions in it, are or are not "self-executing". The latter means "that the treaty has automatic domestic effect as federal law upon ratification." (*Medellin*, 128 S. Ct. at 1356 n.2 (U.S. 2008)). Garcia explains this further:

> Some provisions of international treaties or executive agreements are considered "self-executing," meaning that they have the force of law without the need for subsequent congressional action. Treaty provisions that are not considered self-executing are understood to require implementing legislation to provide U.S. agencies with legal authority to carry out the functions and obligations contemplated by the agreement or to make them enforceable in court by private parties. Treaties have been found to be non-self-executing for at least three reasons: (1) the agreement manifests an intention that it shall not become effective as domestic law without the enactment of implementing legislation; (2) the Senate in giving consent to a treaty, or Congress by resolution, requires implementing legislation; or (3) implementing legislation is constitutionally required. There is significant scholarly debate regarding the distinction between self-executing and non-self-executing agreements, including the ability of U.S. courts to apply and enforce them.
>
> Until implementing legislation is enacted, existing domestic law concerning a matter covered by an international agreement that is not self-executing remains unchanged and controlling law in the United States. However, when a treaty is ratified or an executive agreement is entered into, the United States acquires obligations under international law and may be in default of those obligations unless implementing legislation is enacted.
>
> (Garcia, p. 5, references omitted)

Ratified self-executing treaties and Congressional Executive Agreement are law of the land, equal to federal law and superior to state law, but inferior to the Constitution. In line with this, they override previous federal law but can be set aside or limited by later federal law. In the case of treaties and executive agreements that are not self-executing, it is the implementing legislation that is controlling domestically, not the agreements or treaties themselves. (Garcia, p. 7, references omitted).

9. ***Comment***: There would, in my opinion, be problems with the question of whether (some or indeed perhaps many of) the specific provisions of the EU – US Agreement could be made "self-executing". First of all, if it were to be made an aim of the EU to achieve this, it would mean that those provisions would have to be spelled out very precisely. It is difficult to see how broadly-phrased general principles ("fair", "legitimate", etc.) can be made self-executing. The US courts could either hold quite simply that the stipulations in the Agreement are not self-executing, or apply the relevant principles in the same loose, ineffective way they have applied the rules in the US federal laws: cf. the seemingly similar but in practice fundamentally different application of the "compatible use" criterion in the EU Directive and the "routine uses" exception in the US Privacy Act. Both options for the US courts would be bad from an EU perspective; the latter would probably be worse.

Crucially, if the question of self-executability of (provisions in the) Agreement were to be left unresolved, this would make it even more difficult for individuals from the EU to try and enforce their rights under the Agreement in the US courts. Before they could invoke a provision which they would claim had been breached, they would first have to show that that provision was self-

executing. If this were to be denied by the defending party in the proceedings, the court case would become extremely complex and lengthy, and costly. It would render any remedy in those courts ineffective to EU litigants.

The EU and the USA may wish to avoid this problem altogether, by leaving enforcement entirely to the EU and US supervisory bodies, excluding the courts. However, that would also seriously undermine the worth of the Agreement to individuals whose data were sent from the EU to the USA. Data subjects find it quite hard to obtain serious redress for breaches of their data protection rights through the European DPAs even within the EU: several of those see themselves more as concilliators trying to settle issues amicably rather then as representatives of and advocates for data subjects (see the recent Thematic Study on assessment of data protection measures and relevant institutions, commissioned by the EU Fundamental Rights Agency (FRA), available from: http://www.fra.europa.eu/fraWebsite/attachments/Data-protection_en.pdf).

In this connection , it is also notable that the EU – US "Safe Harbor" arrangement too has rarely, if ever, offered real redress to any European individual. I am not aware of any instance where it has been succesfully relied on by an EU citizen to challenge processing by a US private company, or indeed of any instance when an EU DPA has used it to really challenge practices by any US company, other than in relation to false claims by companies to be members of the scheme.[4] Even in that latter regard, the relevant FTC action was insufficient.[5] Notably, no EU citizen ever seems to have tried to rely on the scheme to assert his or her rights under it - which seems surprising, until one learns that:[6]

> Hundreds of Safe Harbor members belong to very expensive dispute resolution providers, costing thousands of dollars just to lodge a complaint, let alone resolve it. Apparently the FTC does not see this as an issue.

If that system does not really work, what hope is there for the currently proposed public-sector Agreement to be anything more than a fig-leaf?

I am inclined to feel that if the EU wants to go ahead with the idea of an EU – US Agreement in the area we are discussing, it should seek an Agreement that is not self-executing, but rather, one that would require clear, specific implementation by means of a federal law. Of course, the EU could not fully subscribe to the arrangement until it had seen the details of such a (draft) law, and had been able to assess it in terms "adequacy", on the basis of the usual standards, set out in Directive 95/46/EC (and such more specific standards as the data protection rules for Europol and Eurojust etc.). But at least that would mean that the Agreement would be given real "teeth" also in US law, with the sharpness of the teeth (both in substantive and in procedural/protection of individual terms) being fully assessed by EU standards.

In this Note, it should suffice to conclude in this respect that the question of the real, actual legal effect and enforceability of the Agreement in the US legal system, also by EU citizens, is a core issue that should be addressed in the negotiations.

---

[4] This year's *Lane et al. V. Facebook et al.* case could be said to be an exception, but it should be noted that although the FTA was instrumental in the case, and referred to the Safe Harbor undertakings by Facebook in this regard, the case was brought by US citizens and largely resolved (by settlement) under the Video Privacy Protection Act. See: http://www.beaconclasssettlement.com/. On the ineffectiveness of the Safe Harbor arrangements, see the Galexia report of 2008 (especially the summary of findings at pp. 4 – 5), available from: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf

[5] http://www.galexia.com/public/research/articles/research_articles-art56.html.

[6] http://www.galexia.com/public/research/articles/research_articles-art56.html.

III. The effect of an overall EU – US Agreement on exisiting EU – US and Member States – US agreements in the areas of law enforcement and the fight against terrorism

10. The US Ambassador repeatedly stressed that his Government viewed with the greatest concern the possibility that any EU – US Agreement "would have retro-active application". He said that this was probably the US' main concern. He raised in particular the spectre of criminal proceedings already underway in the USA, in which data obtained from the EU (presumably, from an EU MS or several MSs) were relied on, would have to be aborted because the disclosure would be incompatible with the provisions in a new EU – US overall agreement. He also voiced concern that a new EU – US Agreement would somehow immediately invalidate all existing Member State – US Agreements, of which, he said, there are "hundreds" (!).

11. ***Comment:*** As I mentioned in my oral presentation, these are two glaring red herrings:

– First, even in ordinary civil law, contracts and agreements of course do not have retro-active effect (unless they themselves expressly stipulate otherwise). Exactly the same applies to international agreements, as is expressly stipulated in Article 28 ofthe VCLT:

> *Article 28*
> *Non-retroactivity of treaties*
>
> Unless a different intention appears from the treaty or is otherwise established, its provisions do not bind a party in relation to any act or fact which took place or any situation which ceased to exist before the date of the entry into force of the treaty with respect to that party.

If the US is still really concerned about this, it can be expressly spelled out in the EU – US Agreement that that agreement shall not have retro-active effect. There is no problem here whatsoever, and the concerns expressed by the Ambassador in this regard are utterly unfounded. I am surprised he raised them.

– Second, the Agreement would normally have effect from the moment it went into force. This would mean that (unless otherwise provided), the new agreement would override (provisions in) earlier treaties between the same parties covering the same subject matter (Article 30(3) CVLT). Any provisions in any future EU – US Agreement on cooperation in the law enforcement sphere that would cover subject matters already covered in a previous EU – US Agreement would therefore override the provisions on those same subject matters in the earlier agreement (unless otherwise stipulated in the new agreement). This raises difficult questions about what constitutes the "same subject matter". An EU – US Agreement on a subject matter covered in earlier Member State – US Agreements would however not override the provisions in those earlier Member State – US Agreements, because the new agreement is not between the same parties as the earlier agreement (Article 30(4)(b) VCLT).

In simple legal terms, the concerns of the Ambassador in this respect, too, are therefore unfounded: the existing Member State – US Agreements would not be directly legally affected by the proposed new EU – US Agreement. However, from the perspective of the EU at least, the confusing concurring application of possibly conflicting agreements and provisions in agreements (EU – US or Member State – US) would be seriously problematic. The simple answer is to address this in the new Agreement: it should have a section dealing specifically with its effect on existing EU – US and Member States – US Agreements.

12. I have dealt with the way in which that can be done in my Handout, and related it to two further matters: the idea of a "layered" agreement, and the need for a review of the general compatibility of all existing (and new) agreements with the requirements of the the Charter of Fundamental Rights, the ECHR, and the EU *acquis* in the field of data protection.

    On the basic point, it may suffice to reiterate here that in my opinion, this matter should be dealt with by the new Agreement stipulating that that Agreement will (after a suitable implementation/transition period) override previous EU – USA and exisiting Member State – USA agreements on the same subject matter.

    If a "layered" approach were to be adopted (with first a framework agreement being adopted, followed by subsidiary specific agreements on specific data transfers for specific, narrowly-defined purposes), the stipulation should be that (after such a period) the general principles in the framework agreement would override all other existing agreements (EU – US and Member States – US), and that the more specific provisions in the specific (subsidiary) agreements would override corresponding "same subject matter" provisions in any such exisiting agreements.

13. As also already mentioned in my Handout, I feel that given the complexity of the issues (including the question of what constitutes a "same subject matter"), a report should be drawn up to accompany each proposed specific (subsidiary) EU – USA agreement, that lists the relevant Member State – US agreements (or provisions in such agreements) that will be affected (and possibly terminated) by the new specific EU – USA agreement.

14. Finally and more generally, I should repeat here the suggestion in my Handout that the Commission should seek comprehensive information,including the full texts, of all existing arrangements between MSs and the USA in this field, and report to the Council and to Parliament on them, with full disclosure of the texts. The report should include a (non-judicial) assessment of the compatibility of these arrangements with the basic agreement, the Charter of Fundamental Rights, the ECHR, and the EU acquis in the field of data protection. The EU can, in my opinion, take such interest because these arrangements impact on EU-internal and –external arrangements: if some MSs pass on data to the USA, that could affect the operation of intra-EU data flows; and the EU – USA agreements too should take account of the existing Member States – USA agreements.

IV. Summary:

15. Even if the Privacy Act were to be extended to data obtained from the EU (which it clearly will not be), this would not provide "adequate" (let alone "equivalent") protection to European data protection law. But without that, a data sharing agreement that is not itself fully enforceable in the US courts, and that cannot be invoked and relied on by any individual affected by it, in those courts, should be unthinkable.

16. The Agreement, once adopted and ratified, will constitute a "treaty" in the international-legal sense, even though within the USA it would probably take the form of a "Congressional-Executive Agreement" (which is still a treaty in international law).

17. If the EU wants to go ahead with the idea of an EU – US Agreement in the area we are discussing, it should seek an Agreement that is not self-executing, but rather, one that would require clear, specific implementation by means of a federal law. An Agreement that would expressly declare itself to be self-executing would not guarantee proper protection to EU citizens (or others whose data may have been disclosed from the EU to the USA). An Agreement that would leave the question open would if anything be worse.

If the Agreement were to be not self-executing (as I would suggest), it should only come into effect after the EU had assessed the relevant US implementing law as "adequate" in EU data protection terms. It could not and should not come into effect if it were to be judged not "adequate".

18. In any case, the question of the real, actual legal effect and enforceability of the Agreement in the US legal system, also by EU citizens (or others whose data may have been disclosed from the EU to the USA), is a core issue that should be addressed in the negotiations.

19. As also suggested by the EDPS, the Agreement should be given a "layered" structure, consisting of a broad overall basic framework Agreement, within which more specific agreements would be adopted to deal with more specific data exchanges for specific, narrowly-defined purposes within the broad area of law enforcement.

20. The new Agreement should stipulate that that Agreement will (after a suitable implementation/transition period) override previous EU – USA and exisiting Member State – USA agreements on the same subject matter. If a "layered" approach were to be taken, this would mean that similar stipulations should be made, *mutatis mutandis*, in respect of both the main framework Agreement and any subsequent, specific and subsidiary agreements. In that case, a report should be drawn up to accompany each proposed specific (subsidiary) EU – USA agreement, that lists the relevant Member State – US agreements (or provisions in such agreements) that will be affected (and possibly terminated) by the new specific EU – USA agreement.

21. More generally, the Commission should seek comprehensive information,including the full texts, of all existing arrangements between MSs and the USA in this field, and report to the Council and to Parliament on them, with full disclosure of the texts. The report should include a (non-judicial) assessment of the compatibility of these arrangements with the basic agreement, the Charter of Fundamental Rights, the ECHR, and the EU acquis in the field of data protection.

I hope the above summaries and comments may be of use to the LIBE Committee (and others) in their further dealings with the proposed Agreement.

Douwe Korff (Prof.)
Cambridge/London, 29 October 2010